

# PATENT ABSTRACTS OF JAPAN

(11)Publication number :

**09-160492**

(43)Date of publication of  
application :

**20.06.1997**

(51)Int.Cl.

G09C 1/00

H04L 9/32

(21)Application  
number :

**07-324908**

(22)Date of filing :

**13.12.1995**

(71)  
Applicant :

**MATSUSHITA ELECTRIC  
IND CO LTD**

(72)  
Inventor :

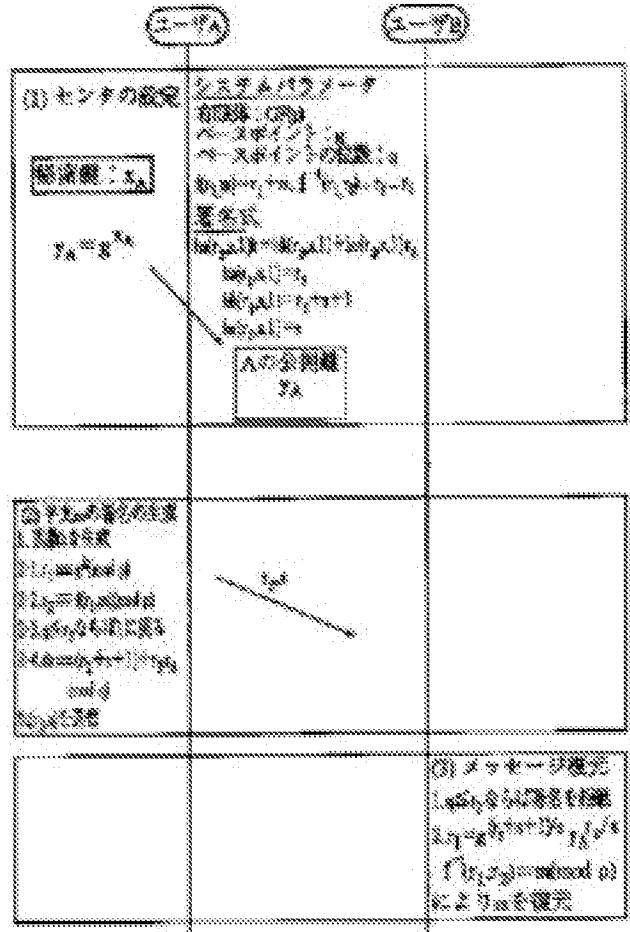
**MIYAJI MITSUKO**

## (54) SIGNATURE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To attain a signature system capable of restoring a message and having high safety.

SOLUTION: Mapping (f) from  $GF(p) \times GF(p)$  to  $GF(p)$  satisfying following tow conditions to  $GF(p)$  is set up as a message masking expression. In the 1st condition, three variables (t), (j), (e) are not replaced by two algebraic expressions in f ( $gtyAj$ ,  $myAe$ ) and  $f(gtyAj, mge)$  in the case of  $GF(p)$  g,  $yA$ , m and  $Zq=\{0, 1, \dots, q-1\}$  t, j, e. In the 2nd condition, the reverse image of  $r2=f(r1, m)$  is  $m=f^{-1}(r1, r2)$ . A signature expression is prepared by mapping  $ha$ ,  $hb$ ,  $hc$  from  $GF(p) \times GF(p) \times GF(p)$  satisfying following expressions [1], [2] to  $GF(p)$ . Where,  $hb(r2', s, 1)-ha(r2', s, 1) \neq hb(rr2', ss, 1)$  when  $ha(r2', s, 1)=ha(rr2', ss, 1)$  and  $hc(r2', s, 1)=hc(rr2', ss, 1)$  [1] and  $hc(r2', s, 1)-ha(r2', s, 1) \neq hc(rr2', ss, 1)$  when  $ha(r2', s, 1)=ha(rr2', ss, 1)$  and  $hb(r2', s, 1)=hb(rr2', ss, 1)$  [2].



(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-160492

(43)公開日 平成9年(1997)6月20日

(51) Int.Cl. <sup>6</sup> G 0 9 C 1/00 H 0 4 L 9/32	識別記号 6 4 0	府内整理番号 7259 -5 J 7259 -5 J 7259 -5 J	F I C 0 9 C 1/00 H 0 4 L 9/00	技術表示箇所 6 4 0 B 6 4 0 D 6 4 0 E 6 7 5 B
---	---------------	---	-------------------------------------	--

審査請求 未請求 請求項の数48 O.L (全23頁)

(21)出願番号 特願平7-324908	(71)出願人 000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日 平成7年(1995)12月13日	(72)発明者 宮地 充子 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
	(74)代理人 弁理士 中島 司朗

## (54)【発明の名称】署名方式

## (57)【要約】

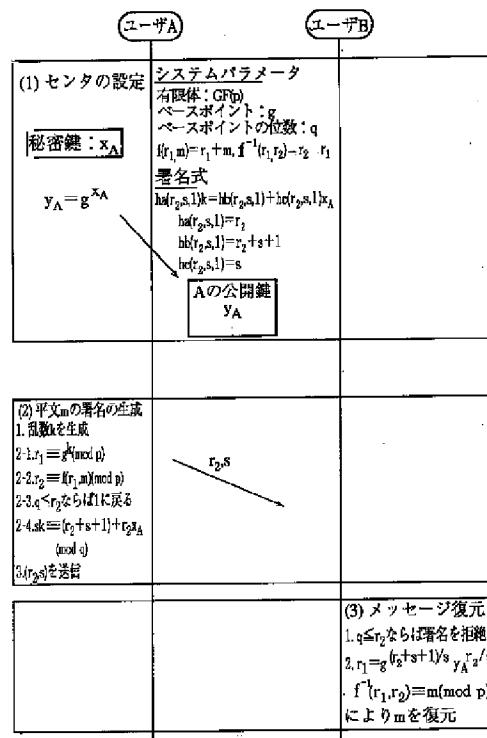
【課題】メッセージ復元が可能かつ安全の高い署名方式を可能とする。

【解決手段】以下の1、2を充たす $GF(p) \times GF(p)$ から $GF(p)$ への写像 $f$ をメッセージマスク式とする。

1:  $GF(p) \ni g, y_A, m, Zq = \{0, 1, \dots, q-1\} \ni t, j, e$ に対し、 $f(g^t y_A^j, my_A^e)$ 及び $f(g^t y_A^j, m)$ において、3変数 $t, j, e$ が2個の代数式で置き換える。

2: 同じく、 $r_2 = f(r_1, m)$ の逆像は $m = f^{-1}(r_1, r_2)$ である。以下の1、2を充たす $GF(p) \times GF(p) \times GF(p)$ から $GF(p)$ への写像 $ha, hb, hc$ にて署名式を作る。

1.  $ha(r_2', s, 1) = ha(rr_2', ss, 1), hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき $hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$
2.  $ha(r_2', s, 1) = ha(rr_2', ss, 1), hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき $hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$



## 【特許請求の範囲】

【請求項1】  $p$  を素数とし、有限体 $GF(p)$  の元を $g$  とし、その位数を $q$  とし、 $GF(p)$  上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、 $k$  を署名者が任意にとる乱数とし、 $r_1 \equiv g^k \pmod{p}$  を署名生成処理におけるコミットメントとし、 $GF(p) \times GF(p)$  から $GF(p)$  への写像を $f$  とするとき、 $r_1$  と $m$  を $f$  により変換した $f(r_1, m)$  を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項2】  $p$  を素数とし、 $r$  を正整数とし、有限体 $GF(p^r)$  の元を $g$  とし、その位数を $q$  とし、 $GF(p^r)$  上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、 $k$  を署名者が任意にとる乱数とし、 $r_1 \equiv g^k \pmod{p}$  をコミットメントとし、 $GF(p^r) \times GF(p^r)$  から $GF(p^r)$  への写像を $f_1$  とし、 $GF(p^r)$  から有限環 $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$  への写像を $\pi$  とするとき、 $r_1$  と $m$  を $f_1$  により変換し、この値を更に $\pi$  を用いて変換した $\pi(f_1(r_1, m))$  を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項3】  $p$  を素数とし、有限体 $GF(p)$  上定義された楕円曲線を $E$  とし、 $E(GF(p))$  の元を $G$  とし、その位数を $q$  とし、 $E(GF(p))$  上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、 $k$  を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, ry)$  をコミットメントとし、 $E(GF(p)) \times GF(p)$  から $GF(p)$  への写像を $F$  とするとき、 $R_1$  と $m$  を $F$  より変換した $F(R_1, m)$  を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項4】  $p$  を素数とし、 $r$  を正整数とし、有限体 $GF(p^r)$  上定義された楕円曲線を $E$  とし、 $E(GF(p^r))$  の元を $G$  とし、その位数を $q$  とし、 $E(GF(p^r))$  上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、 $k$  を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, ry)$  をコミットメントとし、 $E(GF(p^r)) \times GF(p^r)$  から $GF(p^r)$  への写像を $F_1$  とし、 $GF(p^r)$  から有限環 $Z_{p^r}$  への写像を $\pi$  とするととき、 $R_1$  と $m$  を $F_1$  により変換し、この値を更に $\pi$  を用いて変換した $\pi(F_1(R_1, m))$  を用いて署名生成処理におけるメッセージ復元を可能にするメッセージマスク式を構成することを特徴としたメッセージ復元型署名方式。

【請求項5】 写像 $f$  は、 $GF(p) \ni g, y_A$  及び $m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$  及び $e$  に対し、

$f(g^t y_A^j, my_A^e)$  及び $f(g^t y_A^j, mg^e)$  において、3変数 $t, j, e$ が2個の代数式で非置換であることを特徴とした請求項1記載の離散対数問題を用いた署名方式。

【請求項6】 写像 $f$  は、 $GF(p^r) \ni g, y_A$  及び $m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$  及び $e$  に対し、 $f_1(g^t y_A^j, my_A^e)$  及び $f_1(g^t y_A^j, mg^e)$  において、3変数 $t, j, e$  が2個の代数式で非置換であることを特徴とした請求項2記載の離散対数問題を用いた署名方式。

【請求項7】 写像 $F$  は、 $E(GF(p)) \ni G$  及び $y_A$ 、 $GF(p) \ni m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$  及び $e$  に対し、 $F(tG+jY_A, m \times x(eY_A))$  及び $f(tG+jy_A, m \times x(eG))$  において、3変数 $t, j$  及び $e$  が2個の代数式で非置換であることを特徴とした請求項3記載の離散対数問題を用いた署名方式。

【請求項8】 写像 $F_1$  は、 $E(GF(p^r)) \ni G$  及び $y_A$ 、 $GF(p^r) \ni m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$  及び $e$  に対し、 $f(tG+jY_A, m \times x(eY_A))$  及び $f(tG+jy_A, m \times x(eG))$  において、3変数 $t, j, e$  が2個の代数式で非置換であることを特徴とした請求項4記載の離散対数問題を用いた署名方式。

【請求項9】 写像 $f$  は、 $GF(p) \ni r_1, r_2, m, g$  及び $y_A$  に対し、 $r_2 = f(r_1, m)$  の逆像を $m = f^{-1}(r_1, r_2)$  で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して  
 $f^{-1}(r_1/g, r_2) \neq \phi(m, g)$   
及 $b$   $f^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$

となることを特徴とした請求項1記載の離散対数問題を用いた署名方式。

【請求項10】 写像 $f_1$  は、 $GF(p^r) \ni r_1, r_2, m, g, y_A$  に対し、 $r_2 = f_1(r_1, m)$  の逆像を $m = f_1^{-1}(r_1, r_2)$  で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して  
 $f_1^{-1}(r_1/g, r_2) \neq \phi(m, g)$   
及 $b$   $f_1^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$

となることを特徴とした請求項2記載の離散対数問題を用いた署名方式。

【請求項11】 写像 $F$  は、 $E(GF(p)) \ni R_1, Y_A$  及び $G$  並びに $GF(p) \ni m$  及び $r_2$  に対し、 $r_2 = f(R_1, m)$  の逆像を $m = f^{-1}(R_1, r_2)$  で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して

$f^{-1}(R_1/G, r_2) \neq \phi(m, G)$   
及 $b$   $f^{-1}(R_1/Y_A, r_2) \neq \psi(m, Y_A)$

となることを特徴とした請求項3記載の離散対数問題を用いた署名方式。

【請求項12】 写像 $F_1$  は、 $E(GF(p^r)) \ni R_1, Y_A$  及び $G$  並びに $GF(p^r) \ni m$  及び $r_2$  に対し、 $r_2 = f(R_1, m)$  の逆像を $m = f^{-1}(R_1, r_2)$  で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して

$$f^{-1}(R_1-G, r_2) \neq \phi(m, G)$$

$$\text{及び } f^{-1}(R_1-Y_A, r_2) \neq \psi(m, Y_A)$$

となることを特徴とした請求項4記載の離散対数問題を用いた署名方式。

【請求項13】 写像  $f$  は、 $(r, y) \rightarrow r + y$  ( $GF(p)$  上の加算) で定義されることを特徴とした請求項1記載のメッセージ復元型署名方式。

【請求項14】 写像  $f_1$  は、 $(r, y) \rightarrow r + y$  ( $GF(p^r)$  上の加算) で定義されることを特徴とした請求項2記載のメッセージ復元型署名方式。

【請求項15】 写像  $F$  は、橍円曲線の  $x$  座標関数を用いて、 $(R, y) \rightarrow x(R) + y$  ( $GF(p)$  上の加算) で定義されることを特徴とした請求項3記載のメッセージ復元型署名方式。

【請求項16】 写像  $F_1$  は、橍円曲線の  $x$  座標関数を用いて、 $(R, y) \rightarrow x(R) + y$  ( $GF(p^r)$  上の加算) で定義されることを特徴とした請求項4記載のメッセージ復元型署名方式。

【請求項17】 写像  $\pi$  は、 $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$  を  $GF(p^r)$  の  $GF(p)$  上の基底とするとき、 $GF(p^r)$  の元  $x = x_1\alpha_1 + \dots + x_r\alpha_r$  ( $x_1, \dots, x_r \in GF(p)$ ) に対して、

$$\pi(x) = x_1 + x_2 p + \dots + x_r p^{r-1}$$

で定義されることを特徴とした請求項2、同4、同6、同8、同10若しくは請求項12記載のメッセージ復元型署名方式。

【請求項18】  $p$  を素数とし、有限体  $GF(p)$  の元を  $g$  とし、その位数を  $q$  とし、  
 $GF(p)$  上定義される署名方式において、署名者Aの秘密鍵を  $x_A$ 、公開鍵を  $y_A = g^{x_A}$  とし、署名したい文を  $m \in GF(p)$  とするとき、 $k$  を署名者が任意にとる乱数とし、 $r_2$  をコミットメント  $r_1 = g^k$  と  $m$  により計算される  $GF(p)$  の元とし、 $r_2' \equiv r_2 \pmod{q}$  とし、

$ha, hb, hc$  を有限環  $Z_q \times Z_q \times Z_q$  から  $Z_q$  への写像とするとき、署名式を、

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

から  $s$  が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項19】  $p$  を素数とし、 $r$  を正整数とし、有限体  $GF(p^r)$  の元を  $g$  とし、その位数を  $q$  とし、  
 $GF(p^r)$  上定義される署名方式において、署名者Aの秘密鍵を  $x_A$ 、公開鍵を  $y_A = g^{x_A}$  とし、署名したい文を  $m \in GF(p^r)$  とするとき、 $k$  を署名者が任意にとる乱数とし、 $r_2$  をコミットメント  $r_1 = g^k$  と  $m$  により計算される有限環  $Z_{p^r}$  の元とし、 $r_2' \equiv r_2 \pmod{q}$  とし、

$ha, hb, hc$  を有限環  $Z_q \times Z_q \times Z_q$  から  $Z_q$  への写像とするとき、署名式を、

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

q)

から  $s$  が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項20】  $p$  を素数とし、有限体  $GF(p)$  上定義された橍円曲線を  $E$  とし、  
 $E(GF(p))$  の元を  $G$  とし、その位数を  $q$  とし、  
 $E(GF(p))$  上定義される署名方式において、署名したい文を  $m \in GF(p)$  とするとき、  
 $k$  を署名者が任意にとる乱数とし、 $r_2$  をコミットメント  $R_1 = kG$  と  $m$  により計算される  $GF(p)$  の元とし、 $r_2' \equiv r_2 \pmod{q}$  とし、

$ha, hb, hc$  を有限環  $Z_q \times Z_q \times Z_q$  から  $Z_q$  への写像とするとき、署名式を、  
 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$  から  $s$  が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項21】  $p$  を素数とし、 $r$  を正整数とし、有限体  $GF(p^r)$  上定義された橍円曲線を  $E$  とし、  
 $E(GF(p^r))$  の元を  $G$  とし、その位数を  $q$  とし、  
 $E(GF(p^r))$  上定義される署名方式において、署名したい文を  $m \in GF(p^r)$  とするとき、  
 $k$  を署名者が任意にとる乱数とし、 $r_2$  をコミットメント  $R_1 = kG$  と  $m$  により計算される有限環  $Z_{p^r}$  の元とし、 $r_2' \equiv r_2 \pmod{q}$  とし、

$ha, hb, hc$  を有限環  $Z_q \times Z_q \times Z_q$  から  $Z_q$  への写像とするとき、署名式を、  
 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$  から  $s$  が計算できるように構成することを特徴としたメッセージ復元型署名方式。

【請求項22】 写像  $ha, hb, hc$  は、 $r_2', s$  を  $Z_q$  の元とするとき、別途予め固定された所定値を除く任意の  $Z_q$  の元  $rr_2'$ ,  $ss$  に対して、次の二つの条件

1.  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ ,  $hc(r_2', s, 1) = hc(rr_2', ss, 1)$  のとき

$$hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$$

2.  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ ,  $hb(r_2', s, 1) = hb(rr_2', ss, 1)$  のとき

$$hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$$

を満足することを特徴とした請求項18、同19、同20若しくは請求項21記載の離散対数問題を用いた署名方式。

【請求項23】 写像  $ha, hb, hc$  は、  
 $ha(r_2', s, 1) = r_2'$ ,  $hc(r_2', s, 1) = s$  とし、  
 $hb(r_2', s, 1)$  は、

$r_2' = rr_2'$ ,  $s = ss$  のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$  、  
 $r_2' = rr_2'$ ,  $hb(r_2', s, 1) = hb(rr_2', ss, 1)$  のとき、 $s = ss$ 、

$$hb(0, 0, 1) \neq 0,$$

を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項24】 写像  $ha, hb, hc$  は、

$ha(r_2', s, 1) = s$ ,  $hc(r_2', s, 1) = r_2'$  とし、  
 $hb(r_2', s, 1) \neq s$ ,  
 $s=ss$ ,  $r_2'=rr_2'$ , のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$   
 $\wedge$   
 $s=ss$ ,  $hb(r_2', s, 1) = hb(rr_2', ss, 1)$  のとき、 $r_2'=rr_2'$ ,  
 $hb(0, 0, 1) \neq 0$

を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項25】 写像 $ha, hb, hc$ は、  
 $ha(r_2', s, 1) = s$ ,  $hb(r_2', s, 1) = r_2'$  とし、  
 $hc(r_2', s, 1) \neq s$ ,  
 $r_2'=rr_2'$ ,  $s=ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、  
 $s=ss$ ,  $hc(r_2', s, 1) = hc(rr_2', ss, 1)$  のとき、 $r_2'=rr_2'$ ,  
 $hc(0, 0, 1) \neq 0$   
 を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項26】 写像 $ha, hb, hc$ は、  
 $ha(r_2', s, 1) = r_2'$ ,  $hb(r_2', s, 1) = s$  とし、  
 $hc(r_2', s, 1) \neq s$ ,  
 $r_2'=rr_2'$ ,  $s=ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、  
 $r_2'=rr_2'$ ,  $hc(r_2', s, 1) = hc(rr_2', ss, 1)$  のとき、 $s=ss$ ,  
 $hc(0, 0, 1) \neq 0$   
 を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項27】 写像 $ha, hb, hc$ は、  
 $hc(r_2', s, 1) = s$ ,  $hb(r_2', s, 1) = r_2'$  とし、  
 $ha(r_2', s, 1) \neq s$ ,  
 $r_2'=rr_2'$ ,  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$  のとき、 $s=ss$ ,  
 $s=ss$ ,  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$  のとき、 $r_2'=rr_2'$ ,  
 $ha(0, 0, 1) \neq 0$   
 を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項28】 写像 $ha, hb, hc$ は、  
 $hc(r_2', s, 1) = r_2'$ ,  $hb(r_2', s, 1) = s$  とし、  
 $ha(r_2', s, 1) \neq s$ ,  
 $r_2'=rr_2'$ ,  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$  のとき、 $s=ss$ ,  
 $s=ss$ ,  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$  のとき、 $r_2'=rr_2'$ ,  
 $ha(0, 0, 1) \neq 0$   
 を満たすことを特徴とした請求項22記載のメッセージ復元型署名方式。

【請求項29】 写像 $hb(r_2', s, 1)$  は、  
 $hb(r_2', s, 1) = r_2' + s + 1$   
 で定義されることを特徴とした請求項23若しくは請求項24記載のメッセージ復元型署名方式。

【請求項30】 写像 $hb(r_2', s, 1)$  は、  
 $hb(r_2', s, 1) = r_2' \times s + 1$   
 で定義されることを特徴とした請求項23若しくは請求項24記載のメッセージ復元型署名方式。

【請求項31】 写像 $hc(r_2', s, 1)$  は、  
 $hc(r_2', s, 1) = r_2' + s + 1$

で定義されることを特徴とした請求項25若しくは請求項26記載のメッセージ復元型署名方式。

【請求項32】 写像 $hc(r_2', s, 1)$  は、  
 $hc(r_2', s, 1) = r_2' \times s + 1$   
 で定義されることを特徴とした請求項25若しくは請求項26記載のメッセージ復元型署名方式。

【請求項33】 写像 $ha(r_2', s, 1)$  は、 $ha(r_2', s, 1) = 0$ となる解 $(r_2', s)$  がビットの多項式で定まる有限時間で確定できることを特徴とした請求項27若しくは請求項28記載のメッセージ復元型署名方式。

【請求項34】 乱数 $k$  を、メッセージマスク式で計算される $r_2$ と署名式で計算される $s$ に対して、  
 $ha(r_2', s, 1) \neq 0$

であるよう取つてることを特徴とした請求項33記載のメッセージ復元型署名方式。

【請求項35】 写像 $ha(r_2', s, 1)$  は、  
 $ha(r_2', s, 1) = r_2' + s + 1$  であることを特徴とした請求項34記載のメッセージ復元型署名方式。

【請求項36】 写像 $ha(r_2', s, 1)$  は、  
 $ha(r_2', s, 1) = r_2' \times s + 1$  であることを特徴とした請求項34記載のメッセージ復元型署名方式。

【請求項37】  $p$  を素数とし、 $q$  の $1/4$ 以上となる正整数とし、有限体 $GF(p)$  の位数が $q$  となる元を $g$  とし、

$GF(p)$  上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、乱数 $k$  を、コミットメント $r_1 = g^k$  と $m$  により構成される $GF(p)$  の元 $r_2$ が、

$0 < r_2 < q$  となるようにとり、  
 上記範囲を限定された $r_2$ を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項38】  $p$  を素数とし、 $r$  を正整数とし、 $q$  を $p$  と大きさがほぼ同じである、すなわち $p \sim q$  となる正整数とし、有限体 $GF(p^r)$  の位数が $q$  となる元を $g$  とし、

$GF(p^r)$  上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、乱数 $k$  を、コミットメント $r_1 = g^k$  と $m$  により構成される $Z_{pr} = \{0, 1, \dots, p^{r-1}\}$  の元 $r_2$ が、

$0 < r_2 < q$  となるようにとり、  
 上記範囲を限定された $r_2$ を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項39】  $p$  を素数とし、有限体 $GF(p)$  上定義された椭円曲線を $E$  とし、  
 $E(GF(p))$  の元を $G$  とし、その位数を $q$  とし、  
 $E(GF(p))$  上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、乱数 $k$  を、コミットメント $r_1 = g^k$  と $m$  により構成される $GF(p)$  の元 $r_2$ が、  
 $0 < r_2 < q$  となるようにとり、  
 上記範囲を限定された $r_2$ を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項40】  $p$  を素数とし、 $r$  を正整数とし、有限体 $GF(p^r)$  上定義された楕円曲線を $E$  とし、 $E(GF(p^r))$  の元を $G$  とし、その位数を $q$  とし、 $E(GF(p^r))$  上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、乱数 $k$  を、コミットメント $r_1 = g^k$  と $m$  により構成される $Z_{pr} = \{0, 1, \dots, p^{r-1}\}$  の元 $r_2$  が、

$$0 < r_2 < q$$

上記範囲を限定された $r_2$  を署名式に用いることを特徴としたメッセージ復元型署名方式。

【請求項41】 楕円曲線 $E$  は、

元の個数が $p$  となる $GF(p)$  上の楕円曲線を用いることを特徴とした請求項39記載の署名方式。

【請求項42】 署名したい文 $m$  に対し、 $m$  のハッシュ関数値 $hash(m)$  を $m$  の代わりに用いることを特徴とした請求項1、同2、同3、同4、同18、同19、同20、同21、同37、同38、同39若しくは請求項40記載の署名方式。

【請求項43】  $p$  を素数とし、有限体 $GF(p)$  の元を $g$  とし、その位数を $q$  とし、

$GF(p)$  上定義される署名方式において、署名者A の秘密鍵を $x_A$ 、公開鍵を $y_A = g^{xA}$  とし、署名したい文を $m \in GF(p)$  とするとき、 $k$  を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$  とし、

$$r_1' \equiv r_1 \pmod{q}, m' \equiv m \pmod{q}$$

$ha, hb, hc$  を有限環 $Z_q \times Z_q \times Z_q$  から $Z_q$  への写像とするとき、署名式を、

$$ha(r_1', s, m')k \equiv hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$$

から $s$  が計算できるように構成することを特徴とした署名方式。

【請求項44】  $p$  を素数とし、 $r$  を正整数とし、有限体 $GF(p^r)$  の元を $g$  とし、その位数を $q$  とし、

$GF(p^r)$  上定義される署名方式において、署名者A の秘密鍵を $x_A$ 、公開鍵を $y_A = g^{xA}$  とし、署名したい文を $m \in GF(p^r)$  とするとき、 $k$  を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$  とし、 $GF(p^r)$  から有限環 $Z_{pr}$  への写像を $\pi$  とするととき、

$$r_1' \equiv \pi(r_1) \pmod{q}, m' \equiv \pi(m) \pmod{q}$$

$ha, hb, hc$  を有限環 $Z_q \times Z_q \times Z_q$  から $Z_q$  への写像とするとき、署名式を、

$$ha(r_1', s, m')k \equiv hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$$

から $s$  が計算できるように構成することを特徴とした署名方式。

【請求項45】  $p$  を素数とし、有限体 $GF(p)$  上定義された楕円曲線を $E$  とし、

$E(GF(p))$  の元を $G$  とし、その位数を $q$  とし、

$E(GF(p))$  上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、

$k$  を署名者が任意にとる乱数とし、コミットメント $R_1 = kG$  とし、 $E(GF(p))$  から $GF(p)$  への写像を $\rho$  とするとき、

$$r_1' \equiv \rho(R_1) \pmod{q}, m' \equiv m \pmod{q}$$

$ha, hb, hc$  を有限環 $Z_q \times Z_q \times Z_q$  から $Z_q$  への写像とするとき、署名式を、

$$ha(r_1', s, m')k \equiv hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$$

から $s$  が計算できるように構成することを特徴とした署名方式。

【請求項46】  $p$  を素数とし、 $r$  を正整数とし、有限体 $GF(p^r)$  上定義された楕円曲線を $E$  とし、

$E(GF(p^r))$  の元を $G$  とし、その位数を $q$  とし、

$E(GF(p^r))$  上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、

$k$  を署名者が任意にとる乱数とし、コミットメント $R_1 = kG$  とし、 $E(GF(p^r))$  から $GF(p^r)$  への写像を $\rho$  とするとき、 $GF(p^r)$  から有限環 $Z_{pr} = \{0, 1, \dots, p^{r-1}\}$  への写像を $\pi$  とするとき、

$$r_1' \equiv \pi(\rho(R_1)) \pmod{q}, m' \equiv \pi(m) \pmod{q}$$

とし、

$ha, hb, hc$  を有限環 $Z_q \times Z_q \times Z_q$  から $Z_q$  への写像とするとき、署名式を、

$$ha(r_1', s, m')k \equiv hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$$

から $s$  が計算できるように構成することを特徴とした署名方式。

【請求項47】 写像 $\rho$  は、楕円曲線の $x$  座標若しくは $y$  座標関数を用いて、 $R \rightarrow x(R)$  若しくは $R \rightarrow y(R)$  で定義されることを特徴とした請求項45若しくは請求項46記載のメッセージ復元型署名方式。

【請求項48】 写像 $\pi$  は、 $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$  を $GF(p^r)$  の $GF(p)$  上の基底とするとき、 $GF(p^r)$  の元

$$x = x_1\alpha_1 + \dots + x_r\alpha_r \quad (x_1, \dots, x_r \in GF(p))$$

に対して、

$$\pi(x) = x_1 + x_2p + \dots + x_rp^{r-1}$$

で定義されることを特徴とした請求項44及び請求項46記載のメッセージ復元型署名方式。

#### 【発明の詳細な説明】

- 【0001】
- 【0002】

#### 【従来の技術】

(発明の技術的背景) 本願発明に直接関係する技術は、

我が国では未だ必ずしも一般に周知とは言いがたいので、まず、間接的に関係する技術も含めて公開ディジタル通信網を使用した暗号通信技術を広く一般的に説明する。

なお、この秘密通信方式等の一般技術については、わが国では、学術書としては池野信一、小山謙二著「現代暗号理論」電子通信学会発行 1986年、一般向けとしては、一松 信著「暗号の数理」講談社刊1980年に詳しい。

【0003】近年、一般に公開されたディジタル通信回線網を使用して相互に通信を行ったり、有料で放送番組を提供したりすることがさかんになってきている。ところで、一般に公開された通信回線網を使用する場合、第三者による盗聴や詐称、あるいは送信者による送信先の間違いを完全に防止することは困難である。このため、秘密通信方式並びに署名及び認証方式と呼ばれる通信方式が重要なものとなっている。ここに、秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行う方式である。また署名及び認証通信方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。さて、この秘密通信及び署名、認証通信の方式には、公開鍵暗号とよばれる数値を利用した方式がある。そして、この公開鍵暗号による方式は、NTT等の公開ディジタル通信網により、国内外の多数の相手と通信を行う等のごとく通信相手が多い数、しかも通信者が相互に暗号技術について本来的に素人であるとき、通信相手ごとに異なる暗号鍵を容易に管理するための手段であり、現在では多数の通信相手と通信を行うのに不可欠な基盤技術とされている。

【0004】以下、この暗号通信技術の基本的原理と手順と特徴を2、3簡単に説明する。

( 1 ) 有限体上の離散対数問題を使用した秘密通信方式。

なお、これはニイルコブリツ著 “ア コウス イン ナンバア セオリイアンド クリプトグラヒイ” (Neal Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag, 1987) に詳しく述べられている。

(原理)  $p$  を素数、 $g$  をその一の原始根、 $u$  を任意の自然数、 $\alpha$  を  $g$  の  $u$  乗の  $p$  を法とする剰余とする。すなわち、 $g^u \equiv \alpha \pmod{p}$  とする。この場合、 $g$  と  $p$  と  $u$  を与えられたときに  $\alpha$  を求めるのは容易である。しかし、 $p$  が 140 枠程度の素数となると、大型計算機の発達した今日でも、 $g$  と  $p$  と  $\alpha$  から  $u$  を求めるのは困難である。これは丁度、2つの素数  $r$  と  $s$  があるとき  $r$  と  $s$  からその積を求めるのは容易であるが、 $r$  と  $s$  が各 140 枠程度となれば、積は 280 枠となるため、これから素因数分解により  $r$  と  $s$  を求めるのは困難なことに似る。

( 2 ) 楕円曲線上の離散対数問題を使用した秘密通信方式。

【0005】しかしながら、近年の大型計算機の発達を背景にして、数学の理論（類体論の高次相互律、分解法則等）を使用して、 $g$  と  $p$  と  $\alpha$  とから比較的少ない計算

量で  $u$  を求める方法が種々開発されつつある。その対策の一としては、素数  $p$  を 140 枠程度のものではなく 200 枠等充分に大きいものとすることがあげられる。ただし、この場合には、桁数が大きいだけに、送受信に際して必要な計算の絶対量が多くなる等の不都合が生じえる。

【0006】これらのため、楕円曲線を使用した秘密通信方式が開発された。

(原理) 次に  $E\{GF(q)\}$  の性質、すなわち秘密通信の根柢の原理について説明する。 $E\{GF(q)\}$  の位数が大きな素数で割れる元  $BP$  をベースポイント、 $d$  は任意の自然数とする。このとき、 $BP$  と  $d$  から  $d \cdot BP$  を計算する ( $BP$  を  $d$  回加える) のは容易である。しかし、 $E\{GF(q)\}$  の与えられた元  $Q$  と  $BP$  に対して、

$$Q = d \cdot BP$$

となる自然数  $d$  が存在するならば  $d$  を求めよという問題は、計算機の発達した今日でも  $BP$  や  $q$  等が 30 枠程度の自然数となるならば困難である。なお、ここに  $BP$  は、 $p$  を法とする有限体  $GF(p)$  上での  $g$  に相当する役を担うものである。

【0007】以上で、暗号通信の一般技術の概略説明は終了する。

### ( 3 ) 署名、認証通信

次に、本願発明に関係する技術たる署名、認証通信について説明する。有限体上の離散対数問題におけるユーザ  $U$  とユーザ  $V$  の共有鍵  $k_{uv}$  を使用しての秘密通信を例にとるならば、ユーザ  $U$  あるいはユーザ  $V$  にとって、一番最初に確かに相手がユーザ  $V$  あるいはユーザ  $U$  であることを認証すること、すなわち第三者による詐称を排除する必要がある。

【0008】この場合、ユーザ  $U$  とユーザ  $V$  とが面談、書留め郵便等により直接確認する手段もあるが、国際間はもとより国内の通信においても煩雑となる。この解決手段として、通信網による公開された数値情報をを利用して署名、認署を行う技術が開発されている。以下この技術について、2、3紹介する。

(通信網提供者による署名認署) 最初、システム初期設定として、通信網提供者が、その秘密鍵  $X$  と、端末の秘密鍵を生成するためのある秘密鍵生成関数  $S$  を保有し、端末の公開鍵を生成するための所定の公開鍵生成関数  $P$  と、所定の一方向性関数  $F$  と、秘密鍵  $X$  を一方向性関数  $F$  に入力したときの出力値  $Y = F(X)$  を端末情報発行センターの公開情報として公開ディジタル通信網を使用する各ユーザに通知する。

【0009】次に、送信に際して、送信者の正当性の証明を欲するユーザ  $U$  が、その端末固有の識別情報  $ID_u$  と、自分で作成した秘密鍵をもとに作成した公開値をセンターに通知し、その登録を請求する。なお、秘密鍵  $X$  と公開値との間には、 $x = S(x, y, k, ID_u)$  の

関係がある。ここに、 $y = F(k)$ 、また $k$ は乱数値である。

【0010】ユーザUからの請求を受けた通信網提供者が、ユーザUの公開値 $y_u$ を他のユーザに公開する。すなわち、ユーザUは、検証用公開鍵として、その秘密鍵 $x$ を前記一方向性関数Fに入力したときの出力値 $y_u = F(x)$ を生成し、送信相手となるユーザVに対して、自分の公開情報として、その公開値 $y$ と識別情報IDuと $y_u$ を、公開ディジタル通信網を介して転送する。

【0011】ユーザVは、ユーザUからその端末公開情報を転送を受けると、ユーザUの公開鍵として、網提供者の公開情報Yと、ユーザUの公開値 $y$ と、その識別情報IDuとを公開鍵生成関数Pに入力したときの出力値 $C = P(Y, y, IDu)$ を生成するこの上で、生成されたユーザUの公開鍵Cと前記検証用公開鍵 $y_u$ を比較し、一致するか否かを確認する。一致したならば、確かに送信者はユーザUであると認める。

【0012】これにより、ユーザVは網提供者の発行した公開値Yを使用してユーザUから送信されてきた公開鍵を入手しえ、ひいては確かにユーザUから送られてきたものと認められる。以上の概略の手順、必要な構成を図2に示す。なお、認証は必ずしも通信網提供者とは限らないのも勿論である。

【0013】次に、具体的な関数式、関数値としての各鍵の値等としては、Yは、式 $Y \equiv F(X) \equiv g^x \pmod{p}$ 等が用いられ、 $k_u$ は乱数発生機により計算され、 $Y_u$ は、式 $Y_u \equiv g^{k_u} \pmod{p}$ により計算し、 $x_u$ は、式 $x_u \equiv S(X, y_u, k_u, IDu) \equiv X \times y_u + k_u \times IDu \pmod{\phi}$ 、(ここに、 $\phi$ はpのオイラー関数値)等により計算され、 $P_u$ は、式 $P_u = P(Y, y_u, IDu) \equiv (Y \wedge y_u) \times (y_u \wedge IDu) \pmod{p}$

等により計算される。なおここに、オイラーの関数 $\psi$ とは、整数である変数の値より小さいかつその変数と互に素な整数の個数をいい、例えば $\psi(p) = p - 1$ 、 $\psi(6) = 2$ (注、1と5)、 $\psi(10) = 4$ (注、1、3、7、9)である。また、任意の互に素な2つの整数uとvの間には、 $u \wedge \psi(v) - 1 \equiv 0 \pmod{v}$ という関係が常に成立する。例えば、 $3\psi(10) - 1 = 3^4 - 1 = 80 \equiv 0 \pmod{10}$ である。また、素数pについては、必ず $n^p - 1 \equiv 0 \pmod{p}$ となり、この対偶として、任意の整数mについて、何か1つの整数nに対して $n^m - 1 \equiv 0 \pmod{n}$ が成立しないならば、mは素数でないことがわかる。

(第3者による署名、認証) 次に、ユーザUとユーザVとの認証に第三のユーザWを介する方式ものもある。この場合には、ユーザUとユーザW、ユーザVとユーザWとは相互に認証が必要であるが、ユーザUとユーザVとの直接の認証は不要となる。そしてこれは、銀行(ユーザWに相当)を介しての金銭取引等で重要である。

【0014】なお、これら署名、認証の内容、方式については別途本願出願人が、特願平2-324479号「公開鍵生成方法及び装置」等にて開示し、また前掲の現代暗号理論にても種々記載されている周知技術であるため、これ以上の説明は省略する。

#### (4) メッセージ復元署名

次に、署名、認署についての技術の一として、本願発明に直接関係するメッセージ復元型署名について説明する。

【0015】1993年にNyberg-Rueppelにより離散対数問題に安全性の根拠をおくメッセージ復元型署名が発表された。以下に離散対数問題を用いたメッセージ復元型署名のひとつについて述べる。これについて詳しくは、Nyberg and Rueppel, "A new signature scheme based on the DSA giving message recovery", 1st ACM Conf. on Comp. and Comm. Security, 1993 を参照されたい。

(メッセージ復元型署名の従来例) 図3は、従来技術としての、上記Nyberg-Rueppel方式におけるメッセージ復元型署名の手順及び構成を示すものである。

【0016】以下、本図を参照しながら従来例の手順を説明する。

#### (1) センターによる初期設定

$p$ を素数、 $GF(p)$ の元を $g$ としその位数を $q$ とする。センターは、システムパラメータとして $p, q, g$ を全ユーザ、すなわち公開ディジタル通信網に接続された全端末に公開する。

#### (2) ユーザAによる秘密鍵の生成と公開鍵の登録要求の発生。

【0017】署名通信を希望するユーザAが、その端末情報を作成し、これを用いてての秘密鍵と対応する公開鍵も作成し、公開鍵の登録をセンターに要求する。このためユーザAは、乱数 $x_A$ を発生させ、これを自分の秘密鍵 $x_A$ とし、対応する公開鍵を $y_A \equiv gx_A \pmod{p}$ により求める。更にセンターを経由して、全ユーザにユーザAの公開鍵 $y_A$ を公開する。

#### (3) ユーザAによる署名の生成及び送信。

【0018】ユーザBに署名、認署通信の発信を行うユーザAは、以下の処理を行う。

1. 亂数 $k$ を生成させる。
2. 次いで、以下の演算を行う。なお、ここに $m$ は通信文である。

$$r_1 \equiv g^k \pmod{p}$$

$$r_2 \equiv m / r_1 \pmod{p} \dots (a)$$

$$r_2' \equiv r_2 \pmod{q}$$

$$s \equiv k - r_2' \times x_A \pmod{q} \dots (b)$$

を計算する。

【0019】3. ユーザAは $(r_2, s)$ を、ユーザBに送信する。

(4) ユーザBによる受信したメッセージの復元  
ユーザBは、以下の式を計算することにより、メッセー

ジ<sub>m</sub>を復元する。

$$1. g^s y_A^{r_2} r_2 \equiv m \pmod{p}$$

ここで、上記 $r_1$ はコミットメントと呼ばれ、(a)はメッセージマスク式、(b)は署名式と呼ばれる。

【0020】上記従来例は、従来不可能であった離散対数問題に基づくメッセージ復元型署名を可能にする。また署名式(b)は以下のように6(=3!)種類の式に一般化される。

$$\begin{aligned} ak &= b + cx_A \pmod{q}, (a, b, c) = (1, r_2', s) \text{ の置換} \\ (b') \end{aligned}$$

### 【0021】

【発明が解決しようとする課題】しかしながら、この従来例のメッセージ復元型署名に対しては、式が(a)と(b)が簡単なため変形が容易であり、例えば $y_A$ 及ぶ $g$ のべき乗並びに $m$ についての掛け算の式が、3変数より2変数の式に置換しえる等のため近年幾つかの攻撃 recovery-equation attack using  $g$  and  $y_A$ , signature-equation attack using  $g$  and  $y_A$ , and homomorphism attack (各「 $g$ と $y_A$ を使用した再生攻撃」、「 $g$ と $y$

$A$ を使用した署名攻撃」及び「準同型攻撃(選択平文攻撃)」が発表された。これについて詳しくは、宮地充子、「メッセージ復元型署名の弱点1」、電子情報通信学会、情報セキュリティ研究会、1995年7月及びNyberg and Rueppel, "A new signature scheme based on

the DSA giving message recovery", 1st ACM Conf. on Comp. and Comm. Security, 1993及びNyberg and Rueppel, "Message recovery for signature schemes based on the discrete logarithm problem", Advances in cryptology-Proceedings of Eurocrypt'94, Lecture Notes in Computer Science, 950(1995), Springer-Verlag, 182-193を参照されたい。なお、参考までにその攻撃の1つを図4に示す。

【0022】これらに加えて、次に述べる冗長性を利用した攻撃(redundancy attack)が存在する。署名通信等では、解読の困難性からは $p$ 、 $q$ は大きい程好ましいが、必要な演算が少なくて済む等の面からは小さい方が好ましい。このかねあいから実際的には $p$ は512ビット、1024ビット程度の素数が使用されるが、 $q$ は160ビット程度の数が使用される。この場合、上記 $r_2' \equiv r_2 \pmod{q}$ の式では、 $p$ 以下で $r_2'$ 以外にこの式を充たす数 $r_2$ が存在しうる。本説解はこれを利用したものである。

【0023】今、偽者が一つの署名( $r_2, s$ )を手にいれたとき、容易にこの署名文 $m$ が復元できるが、このとき $rr_2 \equiv r_2' + q \pmod{p}$ (ここに、 $r_1 r_2$ とは $r_2$ の偽を意味する。)

$$mm = rr_2 \times (m/r_2) \quad (\text{ここに } m \text{ とは、 } m \text{ の偽を意味する})$$

を計算し、第三者に( $rr_2, s$ )を送信する。これを受け取った第三者は、 $A$ の公開鍵を用いて従来例に示した復元

方法で $mm$ を復元し、 $A$ から送られたと思ってしまう。この結果、偽者は $A$ になりますことができる。

【0024】参考までに、この攻撃の概要を図4に示す。なお、本図の「チルダー」は偽者が署名を生成することを意味する。これら6つの攻撃により、上記従来例のメッセージ復元型署名方式は、署名式の形によらず、ある文の署名の偽造が一組の文と署名のペアを得るだけで可能になり、安全な方式とはいえないとなった。

【0025】そして、これらのこととは、橢円曲線を使用した場合にもあてはまる。以上説明してきたように最近になってメッセージ復元型署名は、その解読方法が考案され、このためこの署名は安全でないことがわかった。この解読方法は従来の署名(メッセージを復元できない署名)には適応できないことがわかっている。しかし、メッセージ復元性は有用な性質であり、この性質を保持しつつ解読が回避できることが望ましいといって、あまり複雑な署名式、メッセージマスク式を採用したりするのは、必要な計算量の減少を図るという面から好ましくない。

【0026】本発明は、この従来例における問題点を鑑みてなされたもので、メッセージ復元性を保ちながら、提案された各種の解読に対して強い、しかも必要な計算量の少ないメッセージ復元型署名方式を提供することを目的とする。

### 【0027】

【課題を解決するための手段】本発明における署名方式は、 $p$ を素数とし、有限体 $GF(p)$ の元を $g$ とし、その位数を $q$ とし、 $GF(p)$ 上定義される署名方式において、署名者 $A$ の秘密鍵を $x_A$ 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p)$ とするとき、 $k$ を署名者が任意にとる乱数とし、コミットメント $r_1 = g^k$ とし、 $r_1' \equiv r_1 \pmod{q}$ 、 $m' \equiv m \pmod{q}$ とし、 $ha, hb, hc$ を有限環 $Z_q \times Z_q \times Z_q$ から $Z_q$ への写像とするとき、署名式を、 $ha(r_1', s, m')k \equiv hb(r_1', s, m') + hc(r_1', s, m')x_A \pmod{q}$ から $s$ が計算できるように構成している。これにより、各種の攻撃を回避する。

【0028】また、本発明におけるメッセージ復元を可能にするメッセージマスク式を使用したメッセージ復元型署名方式は、メッセージマスク式として、 $p$ を素数とし、有限体 $GF(p)$ の元を $g$ とし、その位数を $q$ とし、 $GF(p)$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_1 \equiv g^k \pmod{p}$ を署名生成処理におけるコミットメントとし、 $GF(p) \times GF(p)$ から $GF(p)$ への写像を $f$ とするとき、 $r_1$ と $m$ を $f$ により変換した $f(r_1, m)$ を用いる。これにより、各種の攻撃を回避する。

【0029】また、本発明における署名方式、メッセージ復元型署名方式は、 $E(G(p^r))$ ,  $E(GF(p^r))$ ,  $E(GF(p^r))$ 上でもなされる。

### 【0030】

【発明の実施の形態】従来技術で記載した目的を達成するため、請求項1の発明では、特に $GF(p)$ 上のメッセージ復元型署名において、 $p$ を素数とし、有限体 $GF(p)$ の元を $g$ とし、その位数を $q$ とし、 $GF(p)$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_1 = g^k$ を署名生成処理におけるコミットメントとし、 $GF(p) \times GF(p)$ から $GF(p)$ への写像を $f$ とするとき、 $r_1$ と $m$ を $f$ により変換した $f(r_1, m)$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0031】請求項2の発明では、特に $GF(p^r)$ 上のメッセージ復元型署名において、 $p$ を素数とし、 $r$ を正整数とし、有限体 $GF(p^r)$ の元を $g$ とし、その位数を $q$ とし、 $GF(p^r)$ 上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_1 = g^k$ をコミットメントとし、 $GF(p^r) \times GF(p^r)$ から $GF(p^r)$ への写像を $f_1$ とし、 $GF(p^r)$ から有限環 $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$ への写像を $\pi$ とするとき、 $r_1$ と $m$ を $f_1$ により変換し、この値を更に $\pi$ を用いて変換した $\pi(f_1(r_1, m))$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0032】請求項3の発明では、特に $GF(p)$ 上のメッセージ復元型署名において、 $p$ を素数とし、有限体 $GF(p)$ 上定義された楕円曲線を $E$ とし、 $E(GF(p))$ の元を $G$ とし、その位数を $q$ とし、 $E(GF(p))$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, r_y)$ をコミットメントとし、 $E(GF(p)) \times GF(p)$ から $GF(p)$ への写像を $F$ とするとき、 $R_1$ と $m$ を $F$ により変換した $F(R_1, m)$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0033】請求項4の発明では、特に $E(GF(p^r))$ 上のメッセージ復元型署名において、 $p$ を素数とし、 $r$ を正整数とし、有限体 $GF(p^r)$ 上定義された楕円曲線を $E$ とし、 $E(GF(p^r))$ の元を $G$ とし、その位数を $q$ とし、 $E(GF(p^r))$ 上定義される署名方式において、署名したい文を $m \in GF(p^r)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $R_1 = kG = (r_x, r_y)$ をコミットメントとし、 $E(GF(p^r)) \times GF(p^r)$ から $GF(p^r)$ への写像を $F_1$ とするとき、 $GF(p^r)$ から有限環 $Z_{p^r}$ への写像を $\pi$ とするとき、 $R_1$ と $m$ を $F_1$ により変換し、この値を更に $\pi$ を用いて変換した $\pi(F_1(R_1, m))$ を用いて署名生成処理におけるメッセージ復元を可能にすることを特徴としている。

【0034】請求項5の発明では、特にメッセージ復元型署名の上のrecovery-equation攻撃を回避するため、写像 $f$ は、 $GF(p) \ni g, y_A$ 及び $m$ 、並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び $e$ に対し、 $f(g^t y_A^j, my_A^e)$ 及び $f(g^t y_A^j, mg^e)$ において、3変数 $t, j, e$ が2個の代数式で非置換である（置き換えられない）ことを特徴としている。

【0035】請求項6の発明では、特にメッセージ復元型署名の上のrecovery-equation攻撃を回避するため、写像 $f$ は、 $GF(p^r) \ni g, y_A$ 及び $m$ 並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び $e$ に対し、 $f_1(g^t y_A^j, my_A^e)$ 及び $f_1(g^t y_A^j, mg^e)$ において、3変数 $t, j, e$ が2個の代数式で非置換である（置き換えられない）ことを特徴としている。

【0036】請求項7の発明では、特にメッセージ復元型署名の上のrecovery-equation攻撃を回避するため、写像 $F$ は、 $E(GF(p)) \ni G$ 及び $Y_A$ 、 $GF(p) \ni m$ 並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び $e$ に対し、 $F(tG + jY_A, m \times x(eG))$ 及び $f(tG + jY_A, m \times x(eG))$ において、3変数 $t, j, e$ が2個の代数式で非置換（置き換えられない）ことを特徴としている。

【0037】請求項8の発明では、特に特にメッセージ復元型署名の上のrecovery-equation攻撃を回避するため、写像 $F_1$ は、 $E(GF(p^r)) \ni G$ 及び $Y_A$ 、 $GF(p^r) \ni m$ 並びに $Z_q = \{0, 1, \dots, q-1\} \ni t, j$ 及び $e$ に対し、 $f(tG + jY_A, m \times x(eY_A))$ 及び $f(tG + jY_A, m \times x(eG))$ において、3変数 $t, j, e$ が2個の代数式で非置換（置き換えられない）ことを特徴としている。

【0038】請求項9の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像 $f$ は、 $GF(p) \ni r_1, r_2, m, g$ 及び $y_A$ に対し、 $r_2 = f(r_1, m)$ の逆像を $m = f^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して $f^{-1}(r_1/g, r_2) \neq \phi(m, g)$ 及び $f^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることを特徴としている。

【0039】請求項10の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像 $f_1$ は、 $GF(p^r) \ni r_1, r_2, m, g$ 及び $y_A$ に対し、 $r_2 = f_1(r_1, m)$ の逆像を $m = f_1^{-1}(r_1, r_2)$ で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して $f_1^{-1}(r_1/g, r_2) \neq \phi(m, g)$ 及び $f_1^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$ となることを特徴としている。

【0040】請求項11の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像 $F$ は、 $E(GF(p)) \ni R_1, Y_A$ 及び $G$ 並びに $GF(p) \ni m$ 及び $r_2$ に対し、 $r_2 = f(R_1, m)$ の逆像を $m = f^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して $f^{-1}(R_1 - G, r_2) \neq \phi(m, G)$ 及び $f^{-1}(R_1 - Y_A, r_2) \neq \psi(m, Y_A)$ となることを特徴としている。

【0041】請求項12の発明では、特に特にメッセージ復元型署名の上のhomomorphism攻撃を回避するため、写像 $F_1$ は、 $E(GF(p^r)) \ni R_1, Y_A$ 及び $G$ 並びに $GF(p^r) \ni m$ 及び $r_2$ に対し、 $r_2 = f(R_1, m)$ の逆像を $m = f^{-1}(R_1, r_2)$ で定義するとき、任意の2変数関数 $\phi$ 、 $\psi$ に対して $f^{-1}(R_1 - G, r_2) \neq \phi(m, G)$ 及び $f^{-1}(R_1 - Y_A, r_2) \neq \psi(m, Y_A)$ となることを特徴としている。

【0042】請求項13の発明では、特にメッセージ復

元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像 $f$ は、 $(r, y) \rightarrow r + y$ ( $GF(p)$  上の加算)で定義されることを特徴としている。請求項14の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像 $f_1$ は、 $(r, y) \rightarrow r + y$ ( $GF(p^r)$  上の加算)で定義されることを特徴としている。

【0043】請求項15の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像 $F$ は、楕円曲線のx座標関数を用いて、 $(R, y) \rightarrow x(R) + y$ ( $GF(p)$  上の加算)で定義されることを特徴としている。請求項16の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像 $F_1$ は、楕円曲線のx座標関数を用いて、 $(R, y) \rightarrow x(R) + y$ ( $GF(p^r)$  上の加算)で定義されることを特徴としている。

【0044】請求項17の発明では、特にメッセージ復元型署名の上のrecovery-equation,homomorphism攻撃を回避するため、写像 $\pi$ は、 $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ を $GF(p^r)$ の $GF(p)$ 上の基底とするとき、 $GF(pr)$ の元 $x = x_1\alpha_1 + \dots + x_r\alpha_r$ ( $x_1, \dots, x_r \in GF(p)$ )に対して、 $\pi(x) = x_1 + x_2p + \dots + x_r p^{r-1}$ で定義されることを特徴としている。

【0045】請求項18の発明では、 $GF(p)$ 上のメッセージ復元型署名の上の攻撃を回避するため、 $p$ を素数とし、有限体 $GF(p)$ の元を $g$ とし、その位数を $q$ とし、 $GF(p)$ 上定義される署名方式において、署名者Aの秘密鍵を $x_A$ 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_2$ をコミットメント $r_1 = g^k$ と $m$ により計算される $GF(p)$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 $ha, hb, hc$ を有限環 $Z_q \times Z_q \times Z_q$ から $Z_q$ への写像とするとき、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$ から $s$ が計算できるように構成することを特徴としている。

【0046】請求項19の発明では、特に $GF(p^r)$ 上のメッセージ復元型署名の上の攻撃を回避するため、 $p$ を素数とし、 $r$ を正整数とし、有限体 $GF(p^r)$ の元を $g$ とし、その位数を $q$ とし、 $GF(pr)$ 上定義される署名方式において、署名者Aの秘密鍵を $x_A$ 、公開鍵を $y_A = g^{x_A}$ とし、署名したい文を $m \in GF(p^r)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_2$ をコミットメント $r_1 = g^k$ と $m$ により計算される有限環 $Z_{pr}$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 $ha, hb, hc$ を有限環 $Z_q \times Z_q \times Z_q$ から $Z_q$ への写像とするとき、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$ から $s$ が計算できるように構成することを特徴としている。

【0047】請求項20の発明では、特に $E(GF(p))$ 上のメッセージ復元型署名の上の攻撃を回避するため、 $p$ を素数とし、有限体 $GF(p)$ 上定義された楕円曲線を $E$ と

し、 $E(GF(p))$ の元を $G$ とし、その位数を $q$ とし、 $E(GF(p))$ 上定義される署名方式において、署名したい文を $m \in GF(p)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_2$ をコミットメント $r_1 = g^k$ と $m$ により計算される $GF(p)$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 $ha, hb, hc$ を有限環 $Z_q \times Z_q \times Z_q$ から $Z_q$ への写像とするとき、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$ から $s$ が計算できるように構成することを特徴としている。

【0048】請求項21の発明では、特に $E(GF(p^r))$ 上のメッセージ復元型署名の上の攻撃を回避するため、 $p$ を素数とし、 $r$ を正整数とし、有限体 $GF(p^r)$ 上定義された楕円曲線を $E$ とし、 $E(GF(p^r))$ の元を $G$ とし、その位数を $q$ とし、 $E(GF(p^r))$ 上定義される署名方式において、署名したい文を $m \in GF(pr)$ とするとき、 $k$ を署名者が任意にとる乱数とし、 $r_2$ をコミットメント $r_1 = g^k$ と $m$ により計算される有限環 $Z_{pr}$ の元とし、 $r_2' \equiv r_2 \pmod{q}$ とし、 $ha, hb, hc$ を有限環 $Z_q \times Z_q \times Z_q$ から $Z_q$ への写像とするとき、署名式を、 $ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$ から $s$ が計算できるように構成することを特徴としている。

【0049】請求項22の発明では、特にメッセージ復元型署名の上のsignature-equaion攻撃を回避するため、写像 $ha, hb, hc$ は、 $r_2', s$ を $Z_q$ の元とするとき、予め固定された少數値を除く任意の $Z_q$ の元 $rr_2', ss$ に対して、次の二つの条件1.  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ ,  $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき $hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$ 2.  $ha(r_2', s, 1) = ha(rr_2', ss, 1)$ ,  $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき $hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$ を満足することを特徴としている。

【0050】請求項23の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $ha, hb, hc$ は、 $ha(r_2', s, 1) = r_2'$ ,  $hc(r_2', s, 1) = s$ とし、 $hb(r_2', s, 1)$ は、 $r_2' = rr_2'$ ,  $s = ss$ のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ ,  $r_2' = rr_2'$ ,  $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、 $s = ss$ ,  $hb(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0051】請求項24の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $ha, hb, hc$ は、 $ha(r_2', s, 1) = s$ ,  $hc(r_2', s, 1) = r_2'$ とし、 $hb(r_2', s, 1)$ は、 $s = ss$ ,  $r_2' = rr_2'$ のとき、 $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ ,  $s = ss$ ,  $hb(r_2', s, 1) = hb(rr_2', ss, 1)$ のとき、 $r_2' = rr_2'$ ,  $hb(0, 0, 1) \neq 0$ を満たすことを特徴としている。

【0052】請求項25の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像 $ha, hb, hc$ は、 $ha(r_2', s, 1) = s$ ,  $hb(r_2', s, 1) = r_2'$ とし、 $hc(r_2', s, 1)$ は、 $r_2' = rr_2'$ ,  $s = ss$ のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ ,  $s = ss$ ,  $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ のとき、 $s = ss$ ,  $hc(0, 0, 1) \neq 0$ を満たすことを特徴としている。

$r_2', ss, 1$  のとき、 $r_2' = rr_2' hc(0, 0, 1) \neq 0$  を満たすことを特徴としている。

【0053】請求項26の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha, hb, hcは、 $ha(r_2', s, 1) = r_2'$ 、 $hb(r_2', s, 1) = s$  とし、 $hc(r_2', s, 1)$  は、 $r_2' = rr_2'$ 、 $s = ss$  のとき、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$ 、 $r_2' = rr_2'$ 、 $hc(r_2', s, 1) = hc(rr_2', ss, 1)$  のとき、 $s = ss$ 、 $hc(0, 0, 1) \neq 0$  を満たすことを特徴としている。

【0054】請求項27の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha, hb, hcは、 $hc(r_2', s, 1) = s$ 、 $hb(r_2', s, 1) = r_2'$  とし、 $ha(r_2', s, 1)$  は、 $r_2' = rr_2'$ 、 $ha(r_2', s, 1) = ha(rr_2', ss, 1)$  のとき、 $s = ss$ 、 $s = ss$ 、 $ha(r_2', s, 1) = ha(r_2', ss, 1)$  のとき、 $r_2' = rr_2'$ 、 $ha(0, 0, 1) \neq 0$  を満たすことを特徴としている。

【0055】請求項28の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha, hb, hcは、 $hc(r_2', s, 1) = r_2'$ 、 $hb(r_2', s, 1) = s$  とし、 $ha(r_2', s, 1)$  は、 $r_2' = rr_2'$ 、 $ha(r_2', s, 1) = ha(rr_2', ss, 1)$  のとき、 $s = ss$ 、 $s = ss$ 、 $ha(r_2', s, 1) = ha(r_2', ss, 1)$  のとき、 $r_2' = rr_2'$ 、 $ha(0, 0, 1) \neq 0$  を満たすことを特徴としている。

【0056】請求項29の発明では、特にメッセージ復元型署名のsignature-equation、比例攻撃を回避するため、写像hb( $r_2', s, 1$ ) は、 $hb(r_2', s, 1) = r_2' + s + 1$  で定義されることを特徴としている。請求項30の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像hb( $r_2', s, 1$ ) は、 $hb(r_2', s, 1) = r_2' \times s + 1$  で定義されることを特徴としている。

【0057】請求項31の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像hc( $r_2', s, 1$ ) は、 $hc(r_2', s, 1) = r_2' + s + 1$  で定義されることを特徴としている。請求項32の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像hc( $r_2', s, 1$ ) は、 $hc(r_2', s, 1) = r_2' \times s + 1$  で定義されることを特徴としている。

【0058】請求項33の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha( $r_2', s, 1$ ) は、 $ha(r_2', s, 1) = 0$  となる解( $r_2', s$ ) が有限時間(ビットデータの多項式、すなわち非指數時間)で確定できることを特徴としている。請求項34の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、乱数kを、メッセージマスク式で計算される $r_2$ と署名式で計算されるsに対して、 $ha(r_2', s, 1) \neq 0$  であるように取つてくることを特徴としている。

【0059】請求項35の発明では、特にメッセージ復

元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha( $r_2', s, 1$ ) は、 $ha(r_2', s, 1) = r_2' + s + 1$  であることを特徴としている。請求項36の発明では、特にメッセージ復元型署名の上のsignature-equation、比例攻撃を回避するため、写像ha( $r_2', s, 1$ ) は、 $ha(r_2', s, 1) = r_2' \times s + 1$  であることを特徴としている。

【0060】請求項37の発明では、特にGF(p) 上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、qを $(P/4) < q$  となる正整数とし、有限体GF(p) の位数がqとなる元をgとし、GF(p) 上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、乱数kを、コミットメント $r_1 = g^k$  とmにより構成されるGF(p) の元 $r_2$ が、 $0 < r_2 < q$  となるようにとり、上記範囲を限定された $r_2$ を署名式に用いることを特徴としている。

【0061】請求項38の発明では、特にGF( $p^r$ ) 上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、qを $(P/4) < q$  となる正整数とし、有限体GF( $p^r$ ) の位数がqとなる元をgとし、GF( $p^r$ ) 上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、乱数kを、コミットメント $r_1 = g^k$  とmにより構成される $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$  の元 $r_2$ が、 $0 < r_2 < q$  となるようにとり、上記範囲を限定された $r_2$ を署名式に用いることを特徴としている。

【0062】請求項39の発明では、特にE(GF(p)) 上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、有限体GF(p) 上定義された楕円曲線をEとし、E(GF(p)) の元をGとし、その位数をqとし、E(GF(p)) 上定義される署名方式において、署名したい文を $m \in GF(p)$  とするとき、乱数kを、コミットメント $r_1 = g^k$  とmにより構成されるGF(p) の元 $r_2$ が、 $0 < r_2 < q$  となるようにとり、上記範囲を限定された $r_2$ を署名式に用いることを特徴としている。

【0063】請求項40の発明では、特にGF( $p^r$ ) 上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、有限体GF( $p^r$ ) 上定義された楕円曲線をEとし、E(GF( $p^r$ )) の元をGとし、その位数をqとし、E(GF( $p^r$ )) 上定義される署名方式において、署名したい文を $m \in GF(p^r)$  とするとき、乱数kを、コミットメント $r_1 = g^k$  とmにより構成される $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$  の元 $r_2$ が、 $0 < r_2 < q$  となるようにとり、上記範囲を限定された $r_2$ を署名式に用いることを特徴としている。

【0064】請求項41の発明では、特にE(GF(p)) 上のメッセージ復元型署名の上の攻撃を回避するため、楕円曲線Eは、元の個数がpとなるGF(p) 上の楕円曲線を用いることを特徴としている。請求項42の発明では、特にメッセージ復元型署名の上の攻撃を回避するため、署名したい文 $m$ に対し、 $m$  のハッシュ関数値hash( $m$ ) を

の代わりに用いることを特徴としている。請求項43の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、有限体GF(p)の元をgとし、その位数をqとし、GF(p)上定義される署名方式において、署名者Aの秘密鍵をx<sub>A</sub>、公開鍵をy<sub>A</sub>=g<sup>x\_A</sup>とし、署名したい文をm ∈ GF(p)とするとき、kを署名者が任意にとる乱数とし、コミットメントr<sub>1</sub>=g<sup>k</sup>とし、r<sub>1</sub>' ≡ r<sub>1</sub> (mod q), m' ≡ m (mod q)とし、ha, hb, hcを有限環Z<sub>q</sub> × Z<sub>q</sub> × Z<sub>q</sub>からZ<sub>q</sub>への写像とするとき、署名式を、ha(r<sub>1</sub>', s, m')k ≡ hb(r<sub>1</sub>', s, m') + hc(r<sub>1</sub>', s, m')x<sub>A</sub> (mod q)からsが計算できるように構成することを特徴としている。

【0065】請求項44の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、有限体GF(p<sup>r</sup>)の元をgとし、その位数をqとし、GF(p<sup>r</sup>)上定義される署名方式において、署名者Aの秘密鍵をx<sub>A</sub>、公開鍵をy<sub>A</sub>=g<sup>x\_A</sup>とし、署名したい文をm ∈ GF(p<sup>r</sup>)とするとき、kを署名者が任意にとる乱数とし、コミットメントr<sub>1</sub>=g<sup>k</sup>とし、GF(p<sup>r</sup>)から有限環Z<sub>p<sup>r</sup></sub>への写像をπとするとき、r<sub>1</sub>' ≡ π(r<sub>1</sub>) (mod q), m' ≡ π(m) (mod q)とし、ha, hb, hcを有限環Z<sub>q</sub> × Z<sub>q</sub> × Z<sub>q</sub>からZ<sub>q</sub>への写像とするとき、署名式を、ha(r<sub>1</sub>', s, m')k ≡ hb(r<sub>1</sub>', s, m') + hc(r<sub>1</sub>', s, m')x<sub>A</sub> (mod q)からsが計算できるように構成することを特徴としている。

【0066】請求項45では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、有限体GF(p)上定義された橍円曲線をEとし、E(GF(p))の元をGとし、その位数をqとし、E(GF(p))上定義される署名方式において、署名したい文をm ∈ GF(p)とするとき、kを署名者が任意にとる乱数とし、コミットメントR<sub>1</sub>=kGとし、E(GF(p))からGF(p)への写像をρとするとき、r<sub>1</sub>' ≡ ρ(R<sub>1</sub>) (mod q), m' ≡ m (mod q)とし、ha, hb, hcを有限環Z<sub>q</sub> × Z<sub>q</sub> × Z<sub>q</sub>からZ<sub>q</sub>への写像とするとき、署名式を、ha(r<sub>1</sub>', s, m')k ≡ hb(r<sub>1</sub>', s, m') + hc(r<sub>1</sub>', s, m')x<sub>A</sub> (mod q)からsが計算できるように構成することを特徴としている。

【0067】請求項46の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、pを素数とし、rを正整数とし、有限体GF(p<sup>r</sup>)上定義された橍円曲線をEとし、E(GF(p<sup>r</sup>))の元をGとし、その位数をqとし、E(GF(p<sup>r</sup>))上定義される署名方式において、署名したい文をm ∈ GF(p<sup>r</sup>)とするとき、kを署名者が任意にとる乱数とし、コミットメントR<sub>1</sub>=kGとし、E(GF(p<sup>r</sup>))からGF(p<sup>r</sup>)への写像をρとするとき、GF(p<sup>r</sup>)から有限環Z<sub>p<sup>r</sup></sub>= {0, 1, ..., p<sup>r</sup>-1}への写像をπとするとき、r<sub>1</sub>' ≡ π(ρ(R<sub>1</sub>)) (mod q), m' ≡ π(m)

(mod q)とし、ha, hb, hcを有限環Z<sub>q</sub> × Z<sub>q</sub> × Z<sub>q</sub>からZ<sub>q</sub>への写像とするとき、署名式を、ha(r<sub>1</sub>', s, m')k ≡ hb(r<sub>1</sub>', s, m') + hc(r<sub>1</sub>', s, m')x<sub>A</sub> (mod q)からs

が計算できるように構成することを特徴としている。

【0068】請求項47の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、写像ρは、橍円曲線のx座標若しくはy座標関数を用いて、R → x(R)若しくはR → y(R)で定義されることを特徴としている。請求項48の発明では、特にE(GF(p))上のメッセージ復元型署名の上の攻撃を回避するため、写像πは、{α<sub>1</sub>, α<sub>2</sub>, ..., α<sub>r</sub>}をGF(p<sup>r</sup>)のGF(p)上の基底とするとき、GF(p<sup>r</sup>)の元x=x<sub>1</sub>α<sub>1</sub> + ... + x<sub>r</sub>α<sub>r</sub> (x<sub>1</sub>, ..., x<sub>r</sub> ∈ GF(p))に対して、π(x)=x<sub>1</sub>+x<sub>2</sub>p+...+x<sub>r</sub>p<sup>r-1</sup>で定義されることを特徴としている。

【0069】

#### 【実施例】

(第1実施例) 以下、本発明を実施例に基づいて説明する。以下、本発明の第1実施例を、図を参照しつつ説明する。まず、公開ディジタル通信網全体の構成について説明する。

【0070】図6は、本発明が実施される公開ディジタル通信網全体の構成図である。本図において、1は通信網提供者である。2は、公開ディジタル通信回線である。2はディジタル通信回線である。3～6は、公開ディジタル通信回線2に接続されたユーザ端末（以下、単に「ユーザ」と言う）A、ユーザB、…、ユーザU、ユーザVである。本図に示すように、通信網提供者は、システムパラメータとして、2進数512ビットで表される素数p、

$$g^q \equiv 1 \pmod{p}$$

となる最小の整数（位数）qが256ビットの整数qである整数g、GF(p)上でf(r<sub>1</sub>, m) ≡ r<sub>1</sub> + m (mod p)そしてその逆字像f<sup>-1</sup>がf<sup>-1</sup>(r<sub>1</sub>, f(r<sub>1</sub>, m)) ≡ m (mod p)を充たすメッセージマスク式f、Zg × Zg × ZgからZgへの写像で、ha(r<sub>2</sub>', s, 1) = s、hb(r<sub>2</sub>', s, 1) ≡ r<sub>2</sub>' + s + 1 (mod q)、hc(r<sub>2</sub>', s, 1)r<sub>2</sub>'を充たす関数ha、hb、hcをシステムパラメータと各ユーザに公開している。

【0071】次に、図6に示す通信網提供者1とユーザ3～6の構成について説明する。図7は、通信網提供者1により提供されたICカードやユーザ自身が作成したパソコン用プログラムの要部の構成図である。本図において、11は秘密鍵作成要求受付部である。12は、秘密鍵発生部である。13は、公開鍵作成部である。14は、公開鍵公開部である。15は、秘密鍵通知形態作成部である。16は、秘密鍵通知部である。

【0072】131は公開鍵作成部13内のgの2<sup>n</sup>のpを法とする剰余記憶部である。132は、同じく法取り出し部である。133は、同じく乗算部である。134は、同じく割算部である。以下、上記各部の作用等について説明する。秘密鍵作成要求受付部11は、各ユ

ザ3～6（本図ではユーザA）からの固有の秘密鍵の作成要求を、ユーザのキーボードを使用しての操作等で受け付ける。秘密鍵発生部12は、秘密鍵作成要求受付部11が受け付けた要求をもとに、内蔵する乱数発生プログラムにより2進数の乱数を発生させ、これを当該ユーザの秘密鍵とする。なお、本実施例では、乱数の発生に際しては、同一の乱数発生を万が一にも防止し、併せて整理の都合もあるため当該ユーザの公開ディジタル通信網上での識別番号をも組み込んだものとしている。またこのため、乱数はpと同じく12ビットとしている。公開鍵作成部13は、2進乱数発生部12の発生させた乱数をもとに公開鍵を作成する。なお、この手順は、後で詳しく説明する。

【0073】公開鍵公開部14は、公開鍵作成部13の作成した公開鍵をその作成要求をなしたユーザ名と共に、全ユーザに公開する。これは、通信網が正当性を承認したユーザ名との公開鍵を対応して登録し、ROM等で発行し、また各ユーザの問い合わせに回答する。秘密鍵通知形態作成部15は、各ユーザの秘密鍵をその操作ミスで外部へ漏出しないよう保護する。秘密鍵通知部16は、秘密鍵を共有鍵の作成等の必要に応じて使用しうるようにする。

【0074】次に、公開鍵作成部13による公開鍵の作成について説明する。公開鍵作成部13は、gの $2^n$ 乗のpを法とする割算部134と法取り出し部132と、乗算部130と乗算部133とを有する。gの $2^n$ のnを法とする割算部131は、g、 $g^2$ 、 $g^4$ 、 $g^8$ …等gの2の累べきのpを法とする割算部134とを有する。g<sub>1</sub>、g<sub>2</sub>…、g<sub>i</sub>をあらかじめ計算して、ROMに記憶している。これを小さい数を例にとって、具体的に示す。p=11、g=2ならば、i=[log<sub>2</sub> 11]=3となり、 $2^3 < 11$ となるため、g、 $g^2$ 、 $g^4$ として2、 $2^2$ 、 $2^4$ を、更に対応するg<sub>1</sub>、g<sub>2</sub>、g<sub>4</sub>として2、4、5を記憶している。法取り出し部132は、秘密鍵発生部12から2進数で表現された秘密鍵の通知を受けると、その値で1が立つ桁に対応するg<sub>1</sub>、g<sub>2</sub>…、g<sub>i</sub>を取り出す。これも、小さい数を例にとって具体的にする。今x a=101（10進の5）とする。1位と3位（各、gの2の0乗と2の2乗）に1が立っている。このためg<sub>1</sub>とg<sub>4</sub>、すなわち2と5を取り出す。乗算部133は、法取り出し部132の取り出した法を掛け合わせる。割算部134は、乗算部133の乗算結果をnで割り、その剰余を求める。上記具体的な数値で示すならば、 $2^{xa} = 2^5 = 2 \times 2^4 \equiv 2 \times 5 \equiv 10 \pmod{11}$ となる。そして、この剰余がユーザAの公開鍵とされる。なお、本実施例でgの累べきを剰余を採用しているのは、 $g^3$ 、 $g^5$ 等の法を採用するのよりも一般的に処理が速く、演算機等も2進で作動することにあわせたものである。

【0075】次に、署名付きの送信を行うユーザA側の

重要な処理の流れを図8に、重要な構成を図9と図10に示す。図9において、31はr<sub>2</sub>制御部である。32は2進乱数発生部である。33はr<sub>1</sub>演算部である。34は、通信文(m)入力部である。35は、f関数部である。36は、q記憶部である。37は、排除部である。また、331は、r<sub>1</sub>演算部内のべき剰余記憶部である。また、332は、同じく法取り出し部である。333は、同じく乗算部である。334は、同じく割算部である。351は、f関数部35内の和算部である。352は、同じく、割算部である。371は、排除部37内のq読み出し出力部371である。372は、同じく引き算部である。373は、同じく比較部である。

【0076】図10において、38はSK部である。381は、SK部38内のk-1演算部である。382は、同じくr<sub>2</sub>+1演算部である。383は、同じくr<sub>2</sub>×<sub>a</sub>演算部である。384は、同じくr<sub>2</sub>+1+r<sub>2</sub>×<sub>a</sub>演算部である。385は、同じく、S計算部である。以下、上記各部の作用等について説明する。

【0077】最初、システムパラメータの入手(a1)と秘密鍵等の作成操作(a2)がなされ、秘密鍵の作成及び公開鍵の登録がなされる(a3)。r<sub>2</sub>制御部31は、署名通信発信にあたり、2進乱数発生部32とm入力部34の作用を調整、制御し、後に説明するが、必要な繰り返し処理をも行う。通信文入力部34は、署名発信のための文、例えば「私は、特発 許明です。電話番号は03-3581-1101。確認願います。」等の文書をユーザにより入力され、これを数値(m)化する(a4)。

【0078】2進乱数発生部32は、コミットメント作成のため署名発信毎に相異なる乱数を発生をさせる。またこのため、発信日時等も乱数発生に使用される。(a5)

r<sub>1</sub>演算部33は、発生された2進乱数kをもとにr<sub>1</sub> $\equiv g^k \pmod{p}$ の演算により、r<sub>1</sub>を求める。このため、通信網提供者におけるgの $2^n$ のpを法とする剰余記憶部131、法取り出し部132、乗算部133、割算部134と同じ構成作用をなす剰余記憶部331、法取り出し部332、乗算部333、割算部334を有している。(a6)

f関数部35は、r<sub>1</sub>演算部33で作成されたr<sub>1</sub>と通信文入力部34で数値化された通信文mをもとに、メッセージマスク式fを使用して、r<sub>2</sub> $\equiv f(r_1, m) \pmod{p}$ の演算を行い、r<sub>2</sub>を求める。(a7)

このため、(mod p)上のr<sub>2</sub> $\equiv r_1 + m$ の和算を行う和算部351と、和のpを法とする剰余を求めるためpでの割算を行う割算部352とを内蔵している。

【0079】q記憶部36は、あらかじめ別途ユーザにより入力されたgをメモリーに記憶している。排除部37は、f関数部35から入力されたr<sub>2</sub>とqとの大小比較を行い(a8)、r<sub>2</sub>がq以上となれば、前述の冗長

攻撃を回避すべくこの送信を行わず、この旨 $r_2$  制御部31に通知する。

【0080】この通知を受けた、 $r_2$  制御部31は、2進乱数発生部32に再度異なる乱数発生をなさしめて(a9)先の $r_1$ と異なる $r_2$ を得、これと通信文入力部34に入力されている通信文mとでf関数を部35にf関数作用させte、先と異なる $r_2$ を求め、更にqとの大小比較を行わしめるというプロセスを、 $g - r_2$ が正となるまで繰り返し実行させる。また、 $q - r_2$ が正となれば、この $r_2$ をSK部37へ出力する。またこのため、排除部37は、q読み出し部371と引き算部372と比較部373とを内蔵している。q読み出し部371は、 $r_2$ の入力があるとq記憶部36からqの値を読み出し、引き算部372に通知する。引き算部372は、通知されたqから $r_2$ の引き算を行う。比較部373は、引き算部372の求めた差が0より小ならば $r_2$ 制御部31へこの旨通知するこのため、この値が正となるまで上述の手順を繰り返し実行されることとなる。また、 $r_2$ が正ならば、入力された $r_2$ をそのままSK部へ通知する。

【0081】SK部38は、署名式 $s \equiv (r_2 + s + 1) + r_2 x_a \pmod{p}$ の演算により、送信対象となるメッセージを作成する(a10)。図14に示すような構成である。そして、内蔵しているk-1演算部381は、2進乱数発生部381にて発生された、そしてそれを使用して計算した $r_2$ の値ががq未満という要件を充たすこととなった乱数kから1を引き去る。なお、この差をaとする。

【0082】同じく、 $r_2 + 1$ 演算部37は、入力された $r_2$ に1を加える。同じく、 $r_2 x_a$ 演算部383は、排除部37から入力された $r_2$ と図示しない秘密鍵記憶部から入力された $x_a$ との積を求める。 $r_2 + 1 + r_2 x_a$ 演算部384は、 $r_2 + 1$ 演算部382から入力された $r_2 + 1$ と $r_2 x_a$ 演算部383から入力された $r_2 x_a$ との和を求める。なお、この和をbとする。s計算部385は、k-1演算部381が求めたaと $r_2 + 1 + r_2 x_a$ 演算部384が求めたbとを使用して、 $s \cdot a \equiv b \pmod{q}$ を充たすsをユークソッドの互除法により求める。そしてこの結果を図示しない送信部へ送る。

【0083】以上のもとで、署名を求める他のユーザBへ、( $r_2$ , s)が署名文として送信されることとなる。(a11)

図11は、署名文を受信したユーザ側の重要な処理の流れを示す図であり、図12は構成図である。本図において、41は受信部である。42は、拒絶部である。43は、q記憶部である。44は、 $y_A$ 記憶部である。45は、 $r_2$ 記憶部である。46は、s記憶部である。47は、g記憶部である。48は、 $r_2 + s + 1$ 演算部である。49は、 $y_A^{1/s} \pmod{p}$ 演算部である。410

は、 $g^s \pmod{p}$ 演算部である。411は、 $y_A^{r_2/s} \pmod{p}$ 演算部である。412は、 $g^{(r_2+1+s)/s} \pmod{p}$ 演算部である。413は、 $r_1 \equiv g^{(r_2+1+s)/s} \pmod{p}$ 演算部である。414は、 $f^{-1}$ 関数部である。

【0084】受信部41は、認署を求める他のユーザ、今Aとする、からの送信文( $r_2$ , s)を受信する(b1)。拒絶部42は、受信があった場合、 $r_2 - q$ を計算し(b2)、正なら一応正当なものとして続行する処理を行うべく他部にこの受信文を流すが、正でなければこの署名を拒否する(b3)。またこのため、送信側ユーザと同じくq記憶部43にあらかじめqを記憶している。 $y_A$ 記憶部44は、通信網提供者より公開された $y_A$ を、あらかじめメモリーに記憶している。

【0085】g記憶部47も、同じくあらかじめgを記憶している。 $r_2$ 記憶部45は、拒絶部42が一応認署した $r_2$ を記憶し、s記憶部46は同じくsを記憶する。なお、 $r_2$ とsの区分けは、別途定めた通信規約に基づきなされる。 $r_2 + s + 1$ 演算部48は、 $r_2$ 記憶部45とs記憶部46からそれぞれ $r_2$ とsを読み出し、和算で $r_2 + s + 1$ を求める。 $y_A^{1/s} \pmod{p}$ 演算部49は、 $y_A$ 記憶部44から $y_A$ を： $S$ 記憶部46からsを読み出して $y_A^{r_2/s} \pmod{p}$ を演算する。 $g^s \pmod{p}$ 演算部410は、s記憶部46からsを、g記憶部47からgを読み出して、 $g^{1/s} \pmod{p}$ を演算する。 $y_A^{(r_2+1+s)/s} \pmod{p}$ 演算部411は、 $r_2$ 記憶部45から読み出した $r_2$ と $y_A^{1/s} \pmod{p}$ を演算部49から読み出した $y_A^{1/s} \pmod{p}$ をもとに、  
( $y_A^{1/s}$ )を $r_2$ 乗し、更にそのpを法とする剰余を求める。 $g^{(r_2+1+s)/s} \pmod{p}$ 演算部412は、 $r_2 + s + 1$ 演算部418から $r_2 + s + 1$ を読み出し、 $g^{1/s} \pmod{p}$ 演算部410から読み出した $g^{1/s} \pmod{p}$ を $r_2 + s + 1$ 乗し、更にこのpを法とする剰余を求める。

【0086】 $r_1 \equiv g^{(r_2+1+s)/s} y_A^{r_2/s} \pmod{p}$ 演算部413は、 $y_A^{r_2/s} \pmod{p}$ 演算部411の演算結果と $g^{(r_2+1+s)/s} \pmod{p}$ 演算部412の演算結果とから、 $r_1 \equiv g^{(r_2+1+s)/s} y_A^{r_2/s} \pmod{p}$ の演算により、 $r_1$ を求める(b4)。 $f^{-1}$ 関数部414は、関数 $f^{-1}$ を使用して演算 $r_2 - r_1$ を行い、mを求める(b5)。

【0087】以上の構成により、ユーザBはユーザAの送信文からm入手するが、この際通信網提供者が公開した $y_A$ に相当する秘密鍵 $x_a$ を知っているのはユーザAのみであり、またこの $x_a$ を使用しない限り $y_A$ を使用しての正しい復号もなしえばい。このため、送信者は、確かにユーザAの署名であると確認する(b6)。次に、以上の説明とかなり重複するが、以上の手順における通信文の処理、各種の数式をもとにしての、式や数値で表現されたデータの変化の様子を中心として、この

手順を説明する。

【0088】図1は、この数値式や面で表現した手順の基本的な構成を示すものである。以下、本図を参照しながら実施例の手順を説明する。

#### (1) センターによる初期設定

$p$  を素数とし、 $GF(p)$  の元を  $g$  としその位数を  $q$  とする。ここで  $p \sim q$  ととる。

【0089】 $GF(p) \times GF(p)$  から  $GF(p)$  への写像  $f$  を、 $f(r_1, m) \equiv r_1 + m \pmod{p}$

$f$  の逆写像  $f^{-1}$  を

$$f^{-1}(r_1, f(r_1, m)) \equiv m \pmod{p}$$

とし、 $Zq \times Zq \times Zq$  から  $Zq$  への写像  $h_a, h_b, h_c$  を、 $h_a(r_2', s, 1) = s, h_c(r_2', s, 1) = r_2'$  とし、 $h_b(r_2', s, 1) \equiv r_2' + s + 1 \pmod{q}$

で定義する。また署名式を

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

で定義する。

【0090】センターは、システムパラメータとして  $p, q, g, f, ha, hb, hc$  を公開する。この状態が、図6に示すものである。

(2) ユーザによる署名送信のための秘密鍵の作成及びセンターが認置した公開鍵の登録。

【0091】ユーザAが、メッセージ復元型署名通信を行うため、その秘密鍵を基に公開鍵を作成し、これを通信網提供者が正しいものとして登録する要求を行う。この要求のため、ユーザAはその端末識別番号を使用して乱数を発生させ、秘密鍵  $X_A$  を生成する。次いで、その公開値  $y_A \equiv g^{X_A} \pmod{p}$  を生成し、生成した公開値はセンターを通じて各ユーザに通知される。

(3) ユーザAによる署名の生成及び送付

1. 2進乱数  $k$  を、プログラムにのっとって生成する。

【0092】2. 以下の演算を順に行う。

$$2-1) r_1 \equiv g^k \pmod{p},$$

$$2-2) r_2 \equiv f(r_1, m) \pmod{p} \dots (c) \text{ とする。}$$

2-3)  $q \leq r_2$  の場合、再度上記1に戻り、異なる2進乱数を生成する。

2-4)  $sk \equiv (r_2 + s + 1) + r_2 x_A \pmod{q} \dots (d)$  より  $s$  を計算する。

【0093】3. 上記2で生成した  $(r_2, s)$  をユーザBに送信する。

(4) ユーザBによる受信したメッセージの復元

1.  $q \leq r_2$  ならば、署名を拒絶する。

2.  $r_1 \equiv g^{(r_2+s+1)/s} y_A^{r_2/s} \pmod{p}$  を計算し、  
 $f^{-1}(r_1, r_2) \equiv m \pmod{p}$

を計算することにより、メッセージ  $m$  を復元する。

【0094】次に、以上の署名の耐攻撃性について説明する。以上の構成のメッセージ復元型署名の場合、コミットメント  $r_1$  が従来例の式(a)のように直接平文  $m$  に関与するのではなく、写像  $f$  を通して関与している。この写

像  $f$  が

(\*)1:  $GF(p) \ni g, y_A$  及び  $m$  並びに  $Zq = \{0, 1, \dots, q-1\}$   $\ni t, j$  及び  $e$  に対し、 $f(g^t y_A^j, my_A^e)$  及び  $f(g^t y_A^j, mg^e)$  において、3変数  $t, j, e$  が2個の代数式で非置換である。このため、recovery equation 攻撃を受けない。

【0095】2:  $GF(p) \ni r_1, r_2, m, g$  及び  $y_A$  に対し、 $r_2 = f(r_1, m)$  の逆像を  $m = f^{-1}(r_1, r_2)$  で定義するとき、任意の2変数関数  $\phi$ ,  $\psi$  に対して  $f^{-1}(r_1/g, r_2) \neq \phi(m, g)$  及び  $f^{-1}(r_1/y_A, r_2) \neq \psi(m, y_A)$  となることから、宮地らにより提案された3つの攻撃(recovery-equation attack, using  $g$  and  $y_A$ , and homomorphism attack)を回避できる。

【0096】また上記実施例のように構成されたメッセージ復元型署名の場合、従来例の式(b')のように署名式の係数  $(a, b, c)$  が  $(r_2', s, 1)$  の置換という形ではなく、写像  $ha, hb, hc$  を用いて決定されている。この写像  $ha, hb, hc$  が  $(**) r_2', s$  を  $Zq$  の元とすると、予め固定された少數値をのぞく全ての  $rr_2', ss$  に対して、次の二つの条件

1.  $ha(r_2', s, 1) = ha(rr_2', ss, 1), hc(r_2', s, 1) = hc(rr_2', ss, 1)$  のとき  $hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$
  2.  $ha(r_2', s, 1) = ha(rr_2', ss, 1), hb(r_2', s, 1) = hb(rr_2', ss, 1)$  のとき  $hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$
- を満たすことから、宮地らにより提案された2つの解読(signature-equation attack using  $g$  and  $y_A$ )を回避できる。さらにこの署名式は従来から存在する比例関係を用いた解読に対しても、署名式が2項に分解されることがないので強い。

【0097】なお、従来から存在する比例関係を用いた比例攻撃に付いては、L. Harn and Y. Xu, "Design of generalised ElGamal type digital signatureschemes based on discrete logarithm", Electron. Lett., Vol. 30(1994), 2025-2026. に詳しい。また、上記実施例のように  $p \sim q$  とすることにより、 $r_2$  の値を制限するステップ(署名生成ではステップ2-3、メッセージ復元ではステップ1)を付加することができる。これにより宮地により提案された1つの解読(redundancy attack)を回避できる。更にこの場合、 $q$  の  $p$  に対する比が従来のごとく  $2^{-400}$  と小さくなく、 $1/3, 1/2$  することにより、再度乱数を発生させ繰り返しての処理を行わねばならない確率も低下しえる。

【0098】なお、上述の実施例は  $f$  を  $r_1 + m$  として行ったが、これは勿論他の写像  $f$  で、(\*)を満たすものなら何でもよい。またこの際、 $r_1 + m$  のように計算量が小さい写像にすることが望ましい。 $ha, hb, hc$  に関するも、上記の性質(\*\*)をもつものなら何でもよい。またこの際、従来から存在する比例関係を用いた解読に対しても強くなるよう、さらに計算量が小さい写像にすることが望ましい。

【0099】また、上記の従来例以外のどんなメッセージ復元型署名にも上記の写像を付加すると同様に解説が回避できる。また、上記の署名方式は、メッセージ $m$ に署名する代わりに、 $m$ にISOで定められたRC-4、RC-2等のハッシュ関数を施したハッシュ値に対して署名し、署名をメッセージとともに送り、ハッシュ値が正しく復元されることをチェックすることで署名を確認するという署名方式としても用いることができる。

【0100】また、上記署名方式は、各ユーザーの秘密鍵等は、通信網提供者又はユーザー用の情報発行センターが生成するものとしたが、これは勿論各ユーザーが任意にその秘密鍵を選定し、公開値等のみセンターへ登録するようにもよい。更に、通信網提供者とユーザー用の情報発行センターが異なってもよい。また、上記署名方式では、各種演算は $GF(p)$ 上でなされるものとしたが、これは勿論 $GF(p^r)$ 上でなされてもよい、この場合には、上記実施例における $(mod p)$ での演算は $(mod p^r)$ での演算となり、このため、 $r_1$ と $m$ を $GF(p^r) \times GF(p^r)$ から $GF(p^r)$ へ字像 $f_1$ を用いて変換した後、この値を更に $GF(p^r)$ から有限環 $Z_{p^r} = \{0, 1, \dots, p^{r-1}\}$ への変更をなす等の手順が付加される。

【0101】なお、この写像 $\pi$ は、 $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ を $GF(p^r)$ の $GF(p)$ 上の基底とすると、 $GF(p^r)$ の元 $x = x_1 \alpha_1 + \dots + x_r \alpha_r$  ( $x_1, x_2, \dots, x_r \in GF(p)$ ) に対して  $\pi(x) = x_1 + x_2 p + \dots + x_r p^{r-1}$  で定義される。この手順を図13に示す。(注、上記実施例は $r=1$ の場合であり、 $\pi$ は恒等写像となり、表面上でこない。)

(第2実施例) 本実施例は、本発明に係るメッセージ復元型署名方式として、橢円曲線上での演算を行うものである。

【0102】本実施例も、基本的な構成、原理は先の第1実施例と異なる。ただし、有限体 $GF(p)$ 上の離散対数問題の困難性ではなく、橢円曲線 $E(GF(p))$ 上の困難性を利用するため、これに関係する点が異なる。このため、この相違する点を中心に説明する。ディジタル公開通信網における通信網提供者1、各ユーザー3~6の接続状態及び初期設定としてのシステムパラメータの概略の構成を図14に示す。

【0103】システムパラメータとして $E(GF(p))$ と、 $g$ に換えての $E(GF(p))$ 上の零元と異なる元 $G$ が加えられ、 $p$ は10進30桁の素数である。これは、 $E(GF(p))$ 上の離散対数問題は有限体上でのそれに比較してはるかに困難であることによる。 $q$ がないが、これは、 $G$ の位数は零元を除き常に $p$ であることによる。また、橢円曲線を使用するため、 $f$ は $x$ 座標関数である。

【0104】各部の構成であるが、第1実施例では、 $p$ を法とする $g^k$ の剩余を計算するため通信網提供者1及

びユーザー側の剩余記憶部131、231等には、 $g$ 、 $g^2$ 、 $g^4$ 、…の $p$ を法とする剩余があらかじめ記憶されていたがこれに換えて、 $G$ 、 $2G$ 、 $4G$ 、…が記憶されているのが大きく異なる。更に、これにあわせて、各種の演算部の乗算も足算を行う点も異なる。

【0105】図15に、通信網提供者の公開鍵作成部213の内部構成を示す。本図に示すように、剩余記憶部2131は、 $G$ 、 $2G$ 、 $4G$ 、 $8G$ …をあらかじめ計算して記憶おり、第1実施例の乗算部13と割算部134に換えて足算部2133を有している。また、これにより、公開鍵として、 $E(GF(p))$ 上の点 $Y_A (= X_A G)$ を計算し、公開する。

【0106】図16に、署名通信を行うユーザーA側の構成を示す。本図においては、32は2進乱数発生部であり、34は、通信文入力部であり、これらは、先の第1実施例と異なる。233は $R_1$ 演算部であり、2進乱数発生部32で発生させた乱数 $k$ 回だけ元 $G$ をえた値 $kG$ を求め、その値 $R_1$ を出力する。このため、あらかじめ、 $2G$ 、 $4G$ 、 $8G$ に対応する $G_2$ 、 $G_4$ 、 $G_8$ 等を記憶している剩余記憶部2331、2進乱数 $k$ の1の立つ桁を取り出す法取り出し部2332、取り出した桁に対応する剩余記憶部2331内の $G_i$ （ここに $i$ は2の乗べき）を取り出し、足し算を行う足し算部2383を内蔵している。

【0107】235は、F関数であり、 $r_2 \equiv m/x (R_1) \pmod{p}$  の演算により $r_2$ を求める。ここに $x (R_1)$ は $R_1$ のX座標値である。238は、求められた $r_2$ と上記乱数 $k$ をもとに、演算 $s \equiv (r_2 + s + 1) + r_2 x_A \pmod{p}$ より $s$ を求めるSK部である。このため、 $k-1 (= a)$ を求める $k-1$ 演算部2381、 $r_2 + 1$ を求める $r_2 + 1$ 演算部2382、 $r_2 x_A$ を求める $r_2 x_A$ 演算部2383、 $r_2 + 1 + r_2 + x_A (= b)$ を求める $r_2 + 1 + r_2 + x_A$ 演算部2384、式 $s \cdot a \equiv b \pmod{p}$ より $s$ を求める $s$ 計算部2385を内蔵している。

【0108】なお、mod演算の法が、 $q$ でなく $p$ であるのが第1実施例と大きく異なる。図17は、受信例ユーザーの構成図である。本図において、受信部41、 $r_2$ 記憶部及び $s$ 記憶部46は第1実施例のものと異なる。247は、あらかじめ $G$ を記憶している $G$ 記憶部である。244は、 $Y_A$ をあらかじめ記憶している $Y_A$ 記憶部である。

【0109】248は、 $r_2$ と $s$ から $(r_2 + s + 1)/s$ を求める $(r_2 + s + 1)/s$ 演算部である。249は、 $r_2/s$ を求める $r_2/s$ 演算部である。2411は、 $E(GF(p))$ 上での演算 $r_2/s Y_A$ を行う $r_2/s Y_A$ 演算部である。2412は、同じく $E(GF(p))$ 上での演算 $((r_2 + s + 1)/s) G$ を行う $((r_2 + s + 1)/s) G$ 演算部である。2413は、同じく、 $E(GF(p))$ 上での演算 $R_1 = ((r_2 + s + 1)/s) G$ を行う $R_1$ 演算部である。

$(r_2 + s + 1) / s \cdot G + (r_2 / s) Y_A$  を行って  $R_1$  を求める演算部である。2414は、演算  $m = x_{(R_1)} r_2$  (ここに、 $x(R_1)$  は  $E(GF(p))$  上の元  $R_1$  の X 座標値) より  $m$  を求める m 演算部である。

【0110】このため、 $q$  と  $r_2$  の大小比較を行う構成がないのも第1実施例と異なる。次に、以上の手順におけるデータそのものの処理、数式、演算を中心とした処理の流れを図18に示す。

#### (1) センターによる初期設定

10進30桁の素数を  $p$  とし、 $GF(p)$  上の元の個数が  $p$  となる橙円曲線を  $E$  とし、 $E(GF(p))$  の元を零元以外の元を  $G$  とする。このときその位数は  $p$  となる。

【0111】 $GF(p) \times GF(p) \times GF(p)$  から  $GF(p)$  への写像  $ha, hb, hc$  を、 $ha(r_2', s, 1) = s, hc(r_2', s, 1) = r_2'$  とし、

$$hb(r_2', s, 1) = r_2' + s + 1 \pmod{q}$$

で定義する。また署名式を

$$ha(r_2', s, 1)k \equiv hb(r_2', s, 1) + hc(r_2', s, 1)x_A \pmod{q}$$

で定義する。

【0112】センターは、システムパラメータとして  $p, E(GF(p)), G, ha, hb, hc$  を全ユーザに公開する。なお、かかる  $E(GF(p))$  の作成手順は、別途本願出願人が前掲の特願平6-134339号等にて開示している技術であるため、その説明は省略する。(2) 署名送信を欲するユーザ A によるそのための秘密鍵の作成及びセンターが認署した公開鍵の登録。

【0113】ユーザ A から、メッセージ復元型署名通信を行うため、その秘密鍵を基に作成した公開鍵を通信網提供者に正しいものとして登録する要求がなされる。このため、ユーザ A は、乱数を発生させ、これを自分の秘密鍵を  $x_A$  とし、対応する公開鍵を橙円曲線  $E(GF(p))$  上での演算  $y_A = x_A G$  により求め、これをセンター経由で全ユーザに公開する。

【0114】併せて秘密鍵  $x_A$  は、ユーザ A が自分のみ秘密に保持するものとする。

#### (3) ユーザ A による署名の生成

ユーザ B に署名発信を行おうとするユーザ A は、以下の処理を行う。

1. 亂数  $k$  を生成する。

2. 2進数の乱数  $k$  を生成する。なお、この乱数は、各送信毎に異なる値がるものとされている。

【0115】2-1)  $E(GF(p))$  上で、演算  $R_1 = KG$  により、 $R_1$  を作成する。

2-2) 法  $p$  上の演算  $r_2 \equiv m / x(R_1) \pmod{p}$  により、 $r_2$  を求める。ここに、 $X(R_1)$  は、 $E(GF(p))$  上の点  $R_1$  の X 座標値である。…(e) とする。

2-3) 法  $p$  上の演算  $sk \equiv (r_2 + s + 1) + r_2 x_A \pmod{p}$  …(f) より  $s$  を計算する。

【0116】3.  $(r_2, s)$  をユーザ B に送信する。

(4) 受信したユーザ B によるメッセージの復元

1. ユーザ A からのメッセージ  $(r_2, s)$  を受信したユーザ B は  $((r_2 + s + 1) / s) G + (r_2 / s) Y_A = R_1$  を  $E(GF(p))$  上で計算し、 $R_1$  を求める。

【0117】2. 次いで、 $m = x(R_1)r_2$  を計算することにより  $m$  を得る。上記実施例のように構成されたメッセージ復元型署名の場合、コミットメント  $R_1$  が従来例の式(a) のように直接平文  $m$  に関与するのではなく、式(e) のように X 座標を通して関与している。すなわち、 $r_2 = F(R_1, m) = m / x(R_1)$  となる。この  $F$  関数が

(\*)1:  $GF(p) \ni g, y_A, m, Z_q = \{0, 1, \dots, q-1\} \ni t, j, e$  に対し、 $F(tG + jY_A, m \times x(eY_A))$  及び  $F(tG + jY_A, m \times x(eG))$ において、3変数  $t, j, e$  が2個の代数式で非置換(置き換えられ)ない。すなわち、 $m \times (eY_A), m \times (eG)$  の偽造攻撃を受けない。

【0118】2:  $E(GF(p)) \ni R_1, G, Y_A, GF(p) \ni r_2, m$  に対し、 $r_2 = F(R_1, m)$  の逆像を  $m = F^{-1}(R_1, r_2)$  で定義するとき、任意の2変数関数  $\phi$ 、 $\phi$  に対して  $F^{-1}(R_1 - G, r_2) \neq \phi(m, G)$  及び  $F^{-1}(R_1 - Y_A, r_2) \neq \phi(m, Y_A)$  となるを満たすことから、宮地らにより提案された3つの解読(recovery-equation attack using g and yA, and homomorphism attack)を回避できる。

【0119】また上記実施例のように構成されたメッセージ復元型署名の場合、従来例の式(b')のように署名式の係数  $(a, b, c)$  が  $(r_2', s, 1)$  の置換という形ではなく、写像  $ha, hb, hc$  を用いて決定されている。この写像  $ha, hb, hc$  が (\*\*\*)  $r_2', s$  を  $Z_q$  の元とするとき、予め固定された少數値をのぞく全ての  $rr_2', ss$  に対して、次の二つの条件

1.  $ha(r_2', s, 1) = ha(rr_2', ss, 1), hc(r_2', s, 1) = hc(rr_2', ss, 1)$  のとき  $hb(r_2', s, 1) - ha(r_2', s, 1) \neq hb(rr_2', ss, 1)$
  2.  $ha(r_2', s, 1) = ha(rr_2', ss, 1), hb(r_2', s, 1) = hb(rr_2', ss, 1)$  のとき  $hc(r_2', s, 1) - ha(r_2', s, 1) \neq hc(rr_2', ss, 1)$
- を満たすことから、宮地らにより提案された2つの解読(signature-equation attack using g and yA)を回避できる。さらにこの署名式は従来から存在する比例関係を用いた解読に対しても、署名式が2項に分解されることがないので強い。なお、従来から存在する比例関係を用いた比例攻撃について、L.Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm", Electron. Lett., Vol.30(1994), 2025-2026. に詳しい。

【0120】また、上記例のような橙円曲線を用いると  $G$  の位数が定義体  $GF(p)$  の  $p$  と等しくなるので、実施例 1 のように  $r_2$  の値を制限するステップを付加することなく、宮地により提案された1つの解読(redundancy attack)を回避できる。また、上述の実施例は X 座標を用いたが、これは勿論他の写像で、(\*) を満たすものなら何でもよい。この際、例えば  $y$  座標のように X 座標と同じ

ように計算量が小さい写像にすることが望ましい。 $ha$ ,  $hb$ ,  $hc$ に関しても、上記の性質(\*\*)をもつものなら何でもよい。またこの際、従来から存在する比例関係を用いた解読に対しても強くなるように、さらに計算量が小さい写像にすることが望ましい。

【0121】また、上記実施例では、定義体 $GF(p)$ の $p$ と $G$ の位数が等しくなるような橙円曲線を用いたが、通常の橙円曲線を用いてもよい。このときには、第1実施例のように $r_2$ を制限するステップを付加する必要がある。また、上記の従来例以外のどんなメッセージ復元型署名にも上記の写像を付加すると同様に解読が回避できる。

【0122】また、第1実施例と同じく、メッセージ $m$ に署名する代わりに、 $m$ にハッシュ関数を施したハッシュ値に対して署名し、署名をメッセージとともに送り、ハッシュ値が正しく復元されることをチェックすることで署名を確認するという署名方式として用いてのよい。また、同じく、 $E(GF(p))$ でなく $E(GF(p^r))$ で行ってもよい。

【0123】また、ユーザは、その秘密鍵等の生成を通じて、通信網提供者にしてもらうようにしてよい。これは、適当な乱数生成器がないときに便利である。以上、本発明を実施例に基づいて説明してきたが、本発明は何も上記実施例に限定されないのは勿論である。

#### 【0124】

【発明の効果】以上、説明してきたように、本発明は、法をメッセージ復元性を保ちながら、官地らにより提案されている従来型のメッセージ復元署名に対する6つの解読法を回避することが可能となり、この一方でそのため付加される計算量も無視できる。このため、公開ディジタル通信網において、安全なメッセージ復元型署名方式を提供することが可能となり、その実用的価値は大きい。

#### 【図面の簡単な説明】

【図1】本発明に係るメッセージ復元型署名の第1実施例の、数値や式の変換を中心とした構成、処理を示した図である。

#### 【図2】従来の署名、認署通信の手順の一例である。

【図3】従来のメッセージ復元型署名の構成を示した図である。

【図4】従来の署名、認署通信に対する公開鍵によるrecovery-equation攻撃の概略手順を示した図である。

#### 【図5】同じく、redundancy攻撃の概略図である。

【図6】本発明に係るメッセージ復元型署名通信が実施される公開ディジタル通信網の概略構成図である。

【図7】上記実施例における、通信網提供者の要部の構成図である。

【図8】同じく、署名通信を行うユーザAの重要な処理の流れを示した図である。

#### 【図9】同じく、署名通信を行うユーザA側の $r_2$ 計算

に係る部分の構成図である。

【図10】同じく、ユーザA側のSK部を中心とした構成図である。

【図11】同じく、署名文を受信したユーザBの重要な処理の流れを示した図である。

【図12】同じく、署名文を受信したユーザB側の要部の構成図である。

【図13】第1実施例の変形例として、 $GF(p)$ でなく $GF(p^r)$ を使用した場合の、関数 $f$ による $GF(p^r)$ から $Z_{pr} = \{0, 1, \dots, p^{r-1}\}$ への変換手順を示した図である。

【図14】本発明に係るメッセージ復元型署名通信の第2実施例が実施される公開ディジタル通信網の概略構成図である。

【図15】上記実施例における、通信網提供者における $E(GF(p))$ 上の演算を実行するための構成である。

【図16】上記実施例における署名文の発行を行うユーザAの構成図である。

【図17】同じく、署名文を受信するユーザBの構成図である。

【図18】同じく、数、値、式の変換を中心とした構成処理を示した図である。

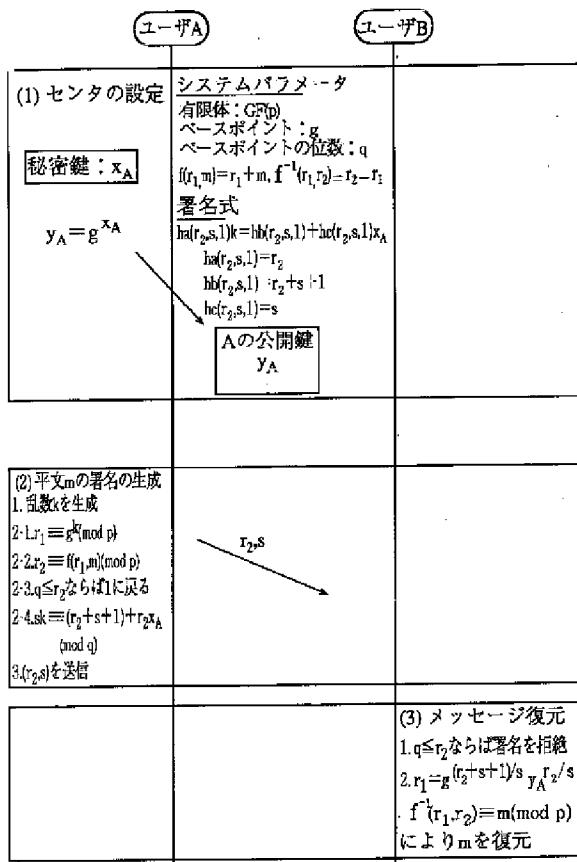
#### 【符合の説明】

- 1 公開ディジタル通信網提供者（各ユーザへの端末情報発行センターを兼ねる。）
- 2 公開ディジタル通信網の回線
- 3、4、5、6、 公開ディジタル通信網に接続されたユーザ
- 1 1 秘密鍵作成要求受付部
- 1 2 秘密鍵発生部
- 1 3 公開鍵作成部
- 1 4 公開鍵公開部
- 1 5 秘密鍵通知形態作成部
- 1 6 秘密鍵通知部
- 3 1  $r_2$  制御部
- 3 2 2進乱数発生部
- 3 3  $r_1$  演算部
- 3 4 通信文入力部
- 3 5 f 関数部
- 3 6 q 関数部
- 3 7 排除部
- 3 7 3 比較部
- 3 8 SK部
- 3 8 5 s 計算部
- 4 1 受信部
- 4 2 拒絶部
- 4 3 q 記憶部（ユーザB）
- 4 4 y<sub>A</sub> 記憶部
- 4 5 r<sub>2</sub> 記憶部

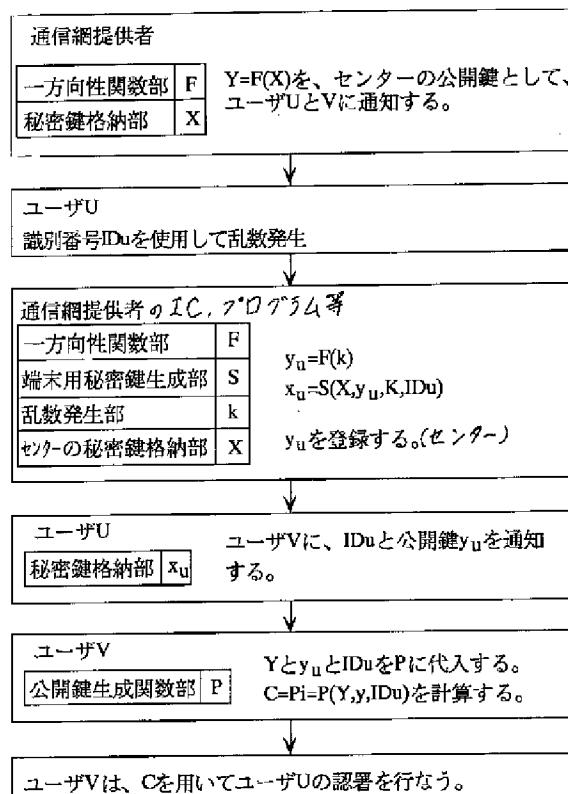
46 s記憶部  
 47 g記憶部  
 413  $r_1 \equiv g^{(r_2+s+1)/s} y_A \mod p$  R2/S (mod p)演算部  
 414 f<sup>-1</sup>関数部  
 2131 剰余記憶部  
 2133 足算部

233 R<sub>1</sub> 演算部  
 235 F関数部  
 238 SK部  
 244 Y<sub>A</sub> 記憶部  
 2413 R<sub>1</sub> 演算部  
 2414 m演算部

【図1】

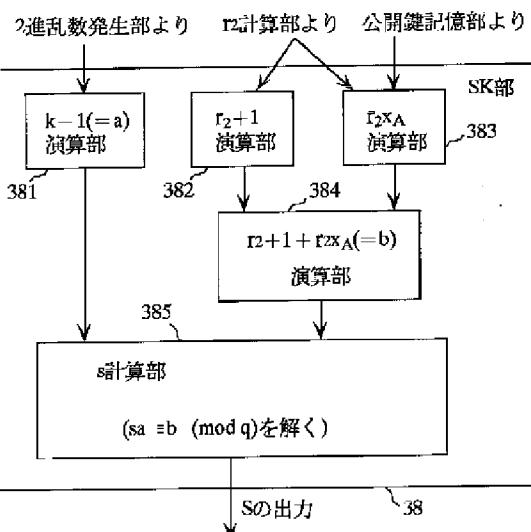
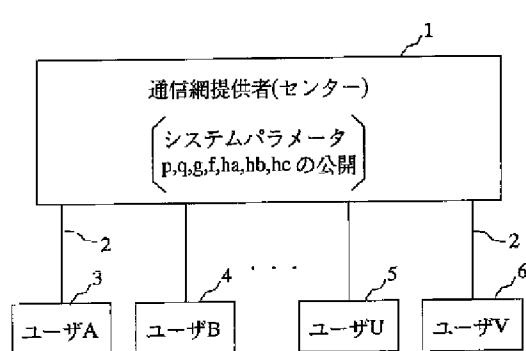


【図2】

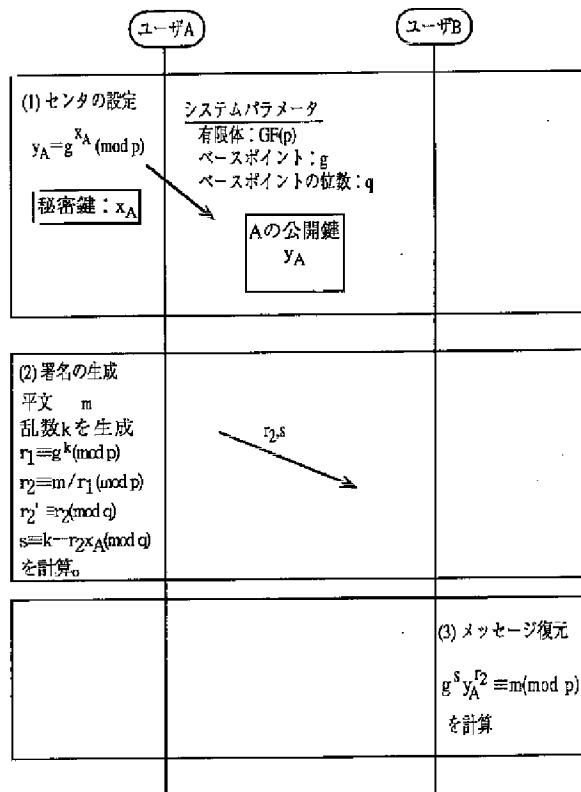


【図10】

【図6】



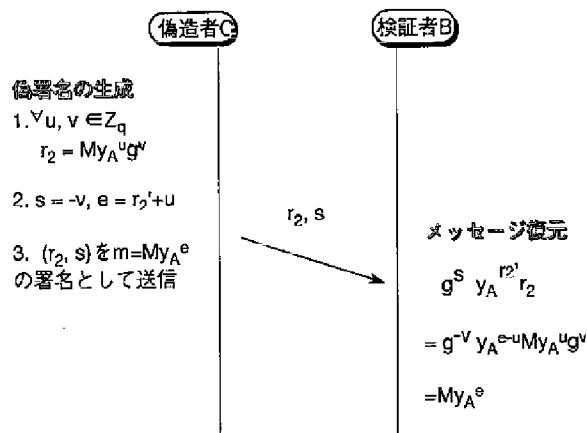
【図3】



【図4】

公開鍵によるrecovery-equation攻撃

予め通信することなく  
 $\forall M \in Z_p$  に対して、  $M y_A^e$  ( $e \in Z_q$ ) の形の平文の偽造ができる

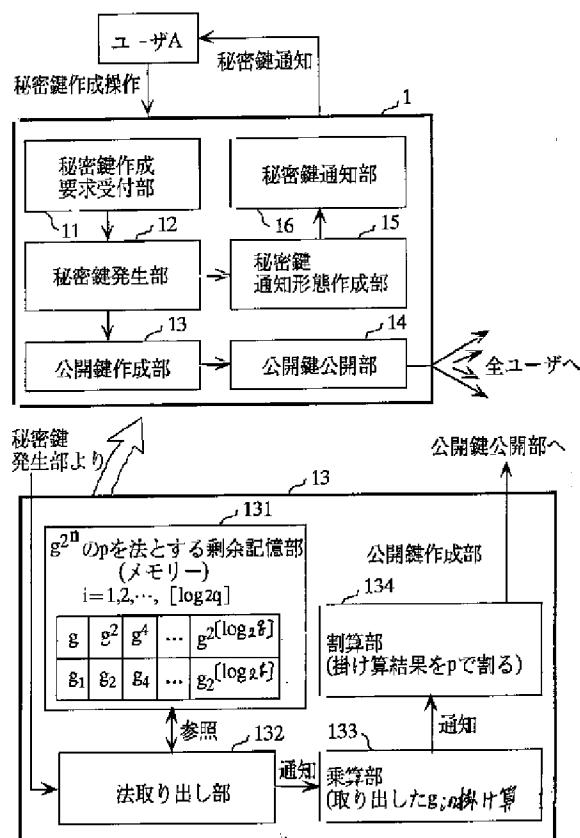
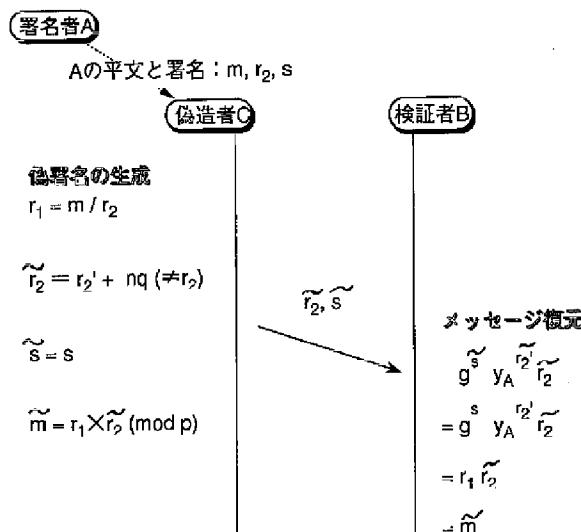


【図7】

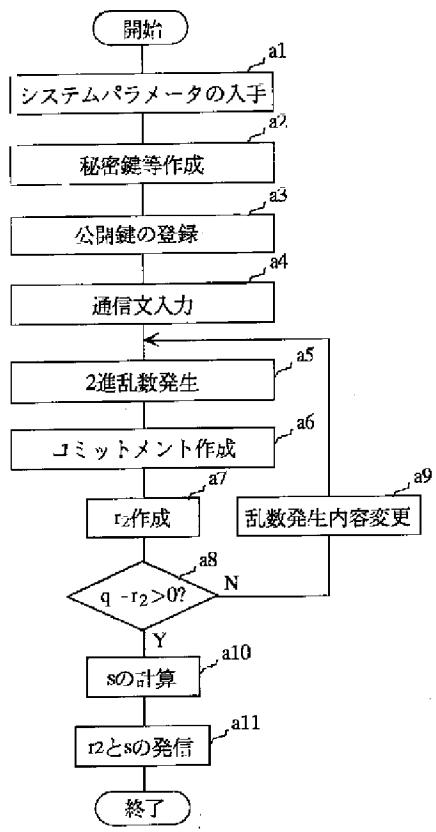
【図5】

redundancy攻撃

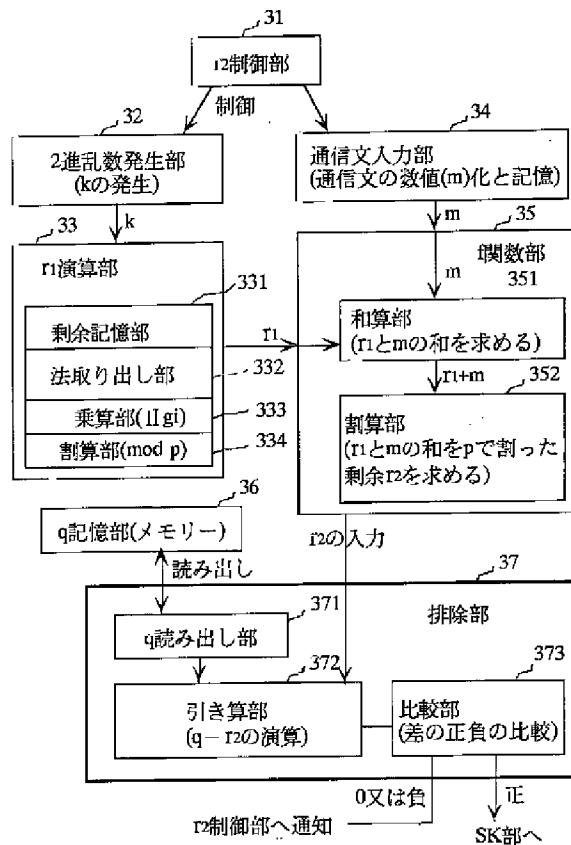
1つの平文と署名のペアを得ると  
新しい平文が偽造できる



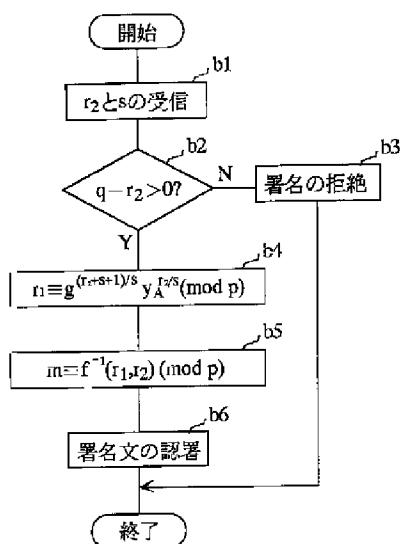
【図8】



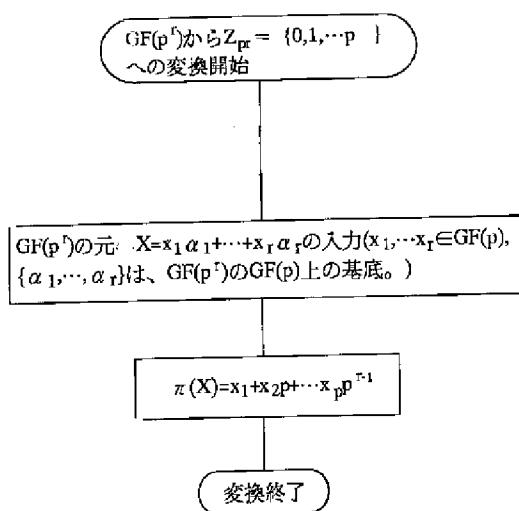
【図9】



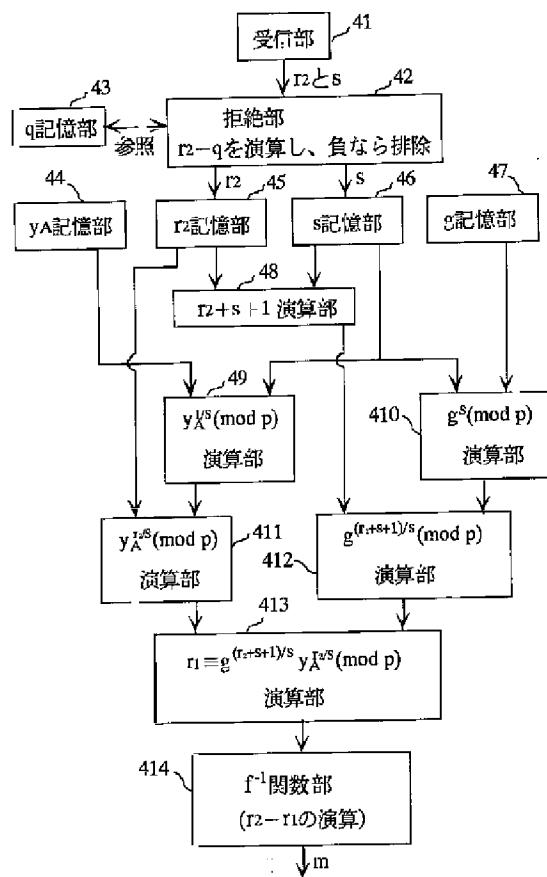
【図11】



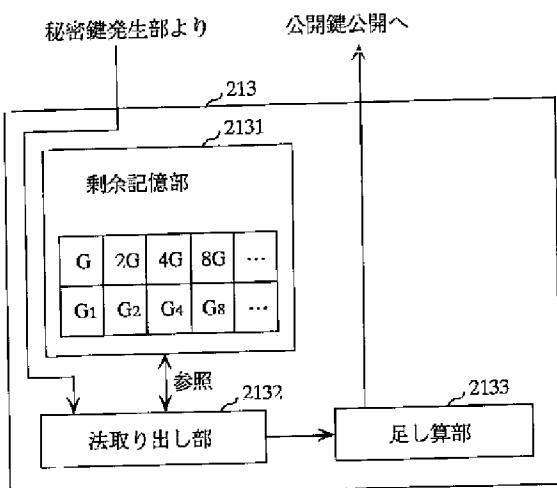
【図13】



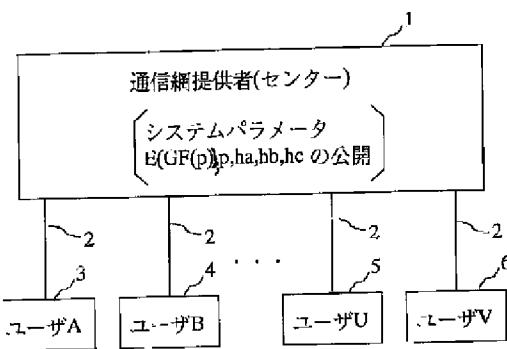
【図12】



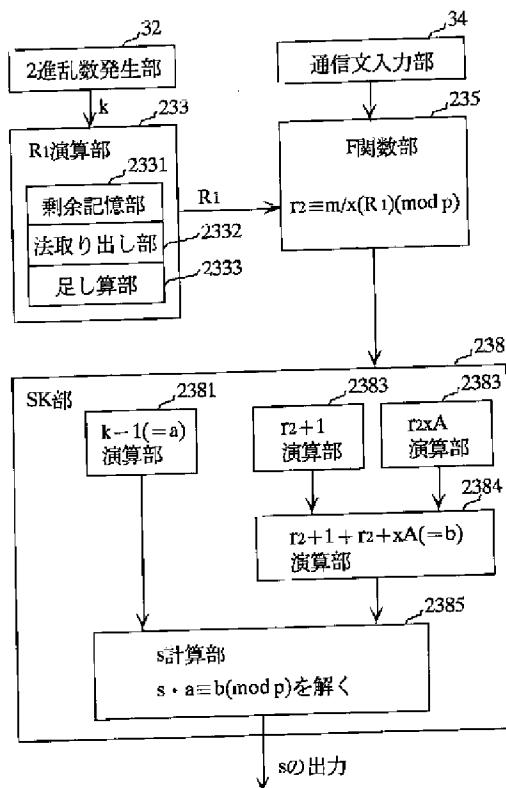
【図15】



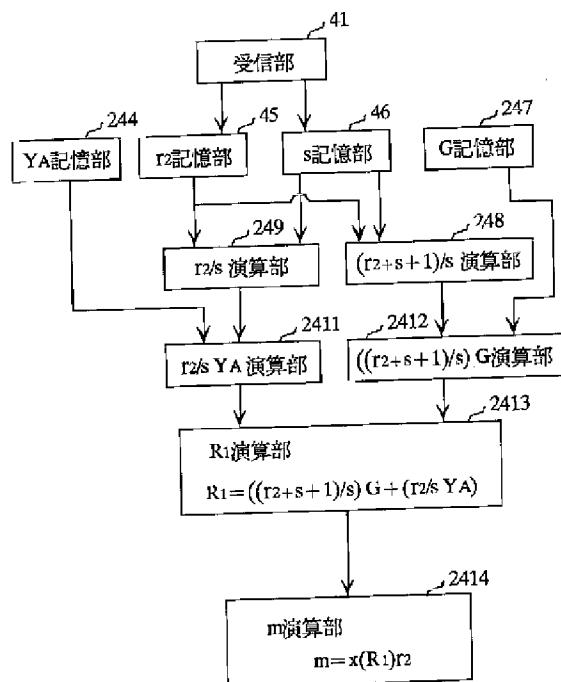
【図14】



【図16】



【図17】



【図18】

